[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00

[12] 发明专利说明书

[21] ZL 专利号 00106192.5

[45] 授权公告日 2004 年 3 月 17 日

[11] 授权公告号 CN 1142653C

[22] 申请日 2000.4.28 [21] 申请号 00106192.5

[71] 专利权人 杨宏伟

地址 100091 北京市海淀区香山路厢红旗 4 号院 6 楼 29 号

[72] 发明人 杨宏伟

审查员 刘剑波

[74] 专利代理机构 北京北新智诚知识产权代理有限公司

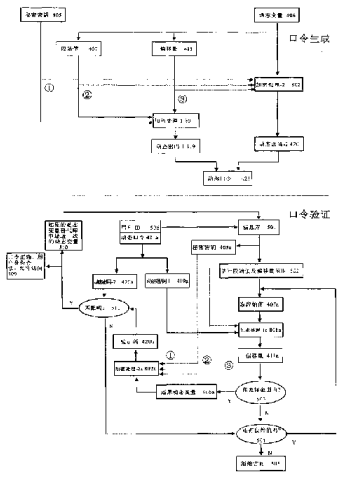
代理人 张卫华

权利要求书 6 页 说明书 20 页 附图 5 页

[54] 发明名称 动态口令认证系统及方法

[57] 摘要

在认证系统中使用的动态口令认证方法，口令生成器用预先给定的段长度和位置对动态变量分段，确定动态变量的段始值和偏移量，对密钥、段始值、偏移量等进行加密处理得出第一动态密码，对密钥、动态变量等进行另一加密处理得出第二动态密码，将第一动态密码和第二动态密码结合生成动态口令；验证口令时，验证器进行相应逆过程处理。 本方法生成的动态口令能隐藏地传递同步信息给验证器，提高了生成动态口令的安全性和验证口令的效率，降低了制作口令生成器的成本。



ISSN1008-4274

知识产权出版社出版

1.一种在由动态口令生成器与验证器构成的动态口令认证系统中使用的动态口令认证方法，动态口令生成器内有第一动态变量和第一秘密密钥，验证器内有第二动态变量和所述动态口令生成器的第二秘密密钥，所述动态口令生成器的第一动态变量和所述验证器的第二动态变量一致地、但独立地产生；其特征在于：

a） 要产生口令时，动态口令生成器的微处理器执行以下步骤：

a1） 根据预先给定的段长度和位置对第一动态变量进行分段，确定第一动态变量的第一段始值和第一偏移量，第一段始值为第一动态变量所在分段的起始位置，第一偏移量为该起始位置至第一动态变量的偏移；

a2） 对第一秘密密钥、第一段始值、第一偏移量进行第一加密处理，得出第一动态密码，该动态密码是第一加密处理的输出结果；对第一秘密密钥、第一动态变量进行第二加密处理，得出第二动态密码，该动态密码是第二加密处理的输出结果；

a3） 将第一动态密码和第二动态密码结合，生成动态口令；

b） 将该动态口令传送至验证器；

c） 要验证口令时，所述验证器的微处理器执行以下步骤：

c1） 分离接收到的动态口令成第三动态密码和第四动态密码；根据预先给定的段长度和位置对第二动态变量进行分段，确定第二动态变量的第二段始值和第二偏移量，第二段始值为第二动态变量所在分段的起始位置，第二偏移量为该起始位置至第二动态变量的偏移；根据第二段始值和第二偏移量确定估计段始值和偏移量范围，估计段始值范围是以所述第二段始值为基础，选取第二段始值及其临近的段始值作为估计段始值，估计偏移量范围是以所述第二偏移量为基础，选取第二偏移量及其临近的偏移量作为估计偏移量；

c2） 对第三动态密码、估计段始值和第二秘密密钥进行第三加密处理，得到第三偏移量，该偏移量是第三加密处理的输出结果；

c3） 若第三偏移量在估计的偏移量范围内，则用第三偏移量和估计段始值还原出第三动态变量，该动态变量是第三偏移量与估计段始值之和；对第二秘密密钥和第三动态变量进行第四加密处理，得到验证码，该验证码是第四加密处理的输出结果；将验证码与第四动态密码比较，若匹配并且该第三动态变量大于最近一次动态变量则用户合法，允许用户访问，验证过程结束；若不匹配或第三偏移量不在估计的偏移量范围内，则判断是否还有另外的估计段始值，若无则用户为非法，拒绝用户访问，验证过程结束；若有则取下一个估计段始值，转步骤c2）。

2.如权利要求1所述的动态口令认证方法，其特征在于：

在所述步骤a2）中，对第一秘密密钥、第一动态变量和第一段始值进行第二加密处理，得出第二动态密码，该动态密码是第二加密处理的输出结果；

在所述步骤c3）中，对第二秘密密钥、第三动态变量和估计段始值进行第四加密处理，得到验证码，该验证码是第四加密处理的输出结果。

3.如权利要求1所述的动态口令认证方法，其特征在于：

在所述步骤a2）中，对第一秘密密钥、第一动态变量、第一段始值和第一偏移量进行

第二加密处理，得出第二动态密码，该动态密码是第二加密处理的输出结果；

在所述步骤c3）中，对第二秘密密钥、第三动态变量、估计段始值和第三偏移量进行第四加密处理，得到验证码，该验证码是第四加密处理的输出结果。

4.如权利要求1所述的动态口令认证方法，其特征在于：

在所述步骤a2）中，第一加密处理包括第一加密算法和第一动态变换表，用第一加密算法作用第一秘密密钥和第一段始值，得出第一动态密钥，该动态密钥是第一加密算法的输出结果，用第一动态密钥产生第一动态变换表，再用第一动态变换表对第一偏移量进行变换，得出第一动态密码，该动态密码是第一动态变换表的输出结果；

在所述步骤c2）中，第三加密处理包括第三加密算法和第二动态变换表，用第三加密算法作用第二秘密密钥和估计段始值，得出第三动态密钥，该动态密钥是第三加密算法的输出结果，用第三动态密钥产生第二动态变换表，再用第二动态变换表对第三动态密码进行变换，得出第三偏移量，该偏移量是第二动态变换表的输出结果。

5.如权利要求4所述的动态口令认证方法，其特征在于：

所述的用第一动态密钥产生第一动态变换表：i → S_i的方法是，这里 $0 \le i < r$，$0 \le S_i < r$，正整数 $r=2^{m1}$，m1 是第一动态密码的比特数，先任意设定 S_i初始状态，并将第一动态密钥按序填入 K_0，K_1，...，K_{r-1}中，可重复利用该密钥，直到填满整个 K_0，K_1，...，K_{r-1}，执行下述动态置换表生成算法：先置 i 和 j 的值为 0，按序执行如下循环操作：a).先将 j 、S_i 和 K_i 的值相加，相加的结果被 r 除后所得的余数再作为 j 的值，b).然后对 S_j和 S_i彼此交换它们各自的值，c).最后将 i 的值增 1，若 i 小于 r 则返回该循环 a)步骤，否则退出该循环操作；由此得到该第一动态变换表：i → S_i；

所述的用第三动态密钥产生第二动态变换表：i → Q_i 的方法是，这里 $0 \le i < r$，$0 \le Q_i < r$，正整数 $r=2^{m1}$，m1 是第一动态密码的比特数，先按前述产生动态变换表步骤，在第三动态密钥作用下产生：i → S_i，其中 $0 \le i < r$，$0 \le S_i < r$，再执行下述程序：先置 i 的值为 0，按序执行如下循环操作：a).先以 S_i的值作为下标，将 i 的值作为 Q_{Si}的值，b).然后将 i 的值增 1，若 i 小于 r 则返回该循环 a)步骤，否则退出该循环操作；由此得到该第二动态变换表：i → Q_i。

6.如权利要求4所述的动态口令认证方法，其特征在于：

所述的用第一动态密钥产生第一动态变换表得出第一动态密码的方法是，由第一动态密钥生成的动态变换表：i → S_i，这里 $0 \le i < r$，$0 \le S_i < r$，正整数 $r=2^{m1}$，m1 是第一动态密码的比特数，k 为第一偏移量，执行下述生成随机码组算法：先置 i 和 j 的值为 0，按序执行如下循环操作：a).先将 j 和 S_i 的值相加，相加的结果被 r 除后所得的余数再作为 j 的值，b).然后对 S_j和 S_i彼此交换它们各自的值，c).最后将 i 的值增 1，若 i 小于 k 则返回该循环 a)步骤，否则退出该循环操作；完成该循环操作后，就将 S_i 和 S_j的值相加，相加的结果被 r 除后所得的余数为 t 值，取 S_t的值为 K，由此得到的 K 作为第一动态密码；

所述的用第三动态密钥产生第二动态变换表得出第三偏移量的方法是，以估计偏移量范围中的每个偏移量值作为k，执行上述生成随机码组算法，得到相应结果K，若K与第三动态密码匹配，则认为k就是所需的第三偏移量。

7.如权利要求2所述的动态口令认证方法，其特征在于：

在所述步骤a2）中，第二加密处理包括第一加密算法和第二加密算法，用第一加密算法作用第一秘密密钥和第一段始值，得出第二动态密钥，该动态密钥是第一加密算法的输出结果，用第二加密算法作用第二动态密钥和第一动态变量，得出第二动态密码，该动态密码是第二加密算法的输出结果；

在所述步骤c3）中，第四加密处理包括第三加密算法和第四加密算法，用第三加密算法作用第二秘密密钥和估计段始值，得出第四动态密钥，该动态密钥是第三加密算法的输出结果，用第四加密算法作用第四动态密钥和第三动态变量，得出验证码，该验证码是第四加密算法的输出结果。

8.如权利要求3所述的动态口令认证方法，其特征在于：

在所述步骤a2）中，第二加密处理包括第一加密算法和第二加密算法，用第一加密算法作用第一秘密密钥和第一段始值，得出第二动态密钥，该动态密钥是第一加密算法的输出结果，将第二动态密钥和第一偏移量结合生成第五动态密钥，再用第二加密算法作用第五动态密钥和第一动态变量，得出第二动态密码，该动态密码是第二加密算法的输出结果；

在所述步骤c3）中，第四加密处理包括第三加密算法和第四加密算法，用第三加密算法作用第二秘密密钥和估计段始值，得出第四动态密钥，该动态密钥是第三加密算法的输出结果，将第四动态密钥和第三偏移量结合生成第六动态密钥，再用第四加密算法作用第六动态密钥和第三动态变量，得出验证码，该验证码是第四加密算法的输出结果。

9.如权利要求4-6之一所述的动态口令认证方法，其特征在于：由第一和第三动态密钥产生的第一和第二动态变换表应大于所述的段长度。

10.如权利要求1-8之一所述的动态口令认证方法，其特征在于：所述第一和第二动态变量分段的方法是，根据预先确定一个段长度和位置，用段长度指定一段内含有多少个偏移量，确定最大偏移量，位置用来指定一段的起点，确定段始值。

11.如权利要求1-8之一所述的动态口令认证方法，其特征在于：所述第一和第二动态变量分别由动态口令生成器和验证器的时钟确定，或者由动态口令生成器已产生口令的次数确定。

12.如权利要求11所述的动态口令认证方法，其特征在于：

若所述第一和第二动态变量由时间确定，则段长度应足以大于动态口令生成器的有效期内，其时钟与验证器时钟之间的最大偏差；

若所述第一和第二动态变量由生成口令的次数确定，则分段的长度应足以大于系统允许、没有由验证器验证、动态口令生成器连续生成的口令个数。

13.如权利要求11所述的动态口令认证方法，其特征在于：

若所述第一和第二动态变量由时间确定，则动态变量应是有一个基本持续时间间隔的预先确定的时间单位的时间值或其函数值；

若所述第一和第二动态变量由生成口令的次数确定，则动态变量应是该次数值或其函数值。

14.如权利要求1-8之一所述的动态口令认证方法，其特征在于：用所述第一加密处理或第一加密算法作用第一段始值之前，对第一段始值进行第一编码，该编码是第一段始值的

表示形式，用所述第二加密处理或第二加密算法作用第一动态变量之前，对第一动态变量进行第二编码，该编码是第一动态变量的表示形式，所述第一编码和第二编码的方式是不同的；用所述第三加密处理或第三加密算法作用估计段始值之前，对估计段始值进行第三编码，该编码是第一段始值的表示形式，用所述第四加密处理或第四加密算法作用第三动态变量之前，对第三动态变量进行第四编码，该编码是第三动态变量的表示形式，所述第三编码和第四编码的方式是不同的。

15.如权利要求1-8之一所述的动态口令认证方法，其特征在于：当所述段长度不大于240时，取第一动态密码和第三动态密码的长度为8比特。

16.如权利要求10所述的动态口令认证方法，其特征在于：所述段长度的选取应使每天所确定的分段位置能够保持一致，位置的最佳选定应是用户频繁使用动态口令生成器时间值的最远点。

17.如权利要求10所述的动态口令认证方法，其特征在于：根据预先确定的段长度和位置，第一动态变量等于第一段始值与某个特定值之积并加上第一偏移量，第二动态变量等于第二段始值与某个特定值之积并加上第二偏移量。

18.如权利要求1-8之一所述的动态口令认证方法，其特征在于：在所述步骤c3）中，若所述的验证码与第四动态密码匹配，将所述第三动态变量与最近一次成功访问所还原的第三动态变量进行比较，若大于该值，则用户合法，允许用户访问，并用所述第三动态变量替代库中保存的最近一次成功访问所还原的第三动态变量，验证过程结束，若不大于该值，则用户非法，拒绝用户访问，验证过程结束。

19.如权利要求1-8之一所述的动态口令认证方法，其特征在于：所选取的估计段始值至少有一个，至多有两个。

20.如权利要求1-8之一所述的动态口令认证方法，其特征在于所述估计段始值和偏移量范围的方法是：

若所述第一和第二动态变量由时间确定，则以第二段始值R和第二偏移量r为基础，依据最近一次的第三动态变量与所述第二动态变量的差值确定应允许的误差范围[c1，c2]，依据最近一次的第三动态变量与最近一次的第二动态变量的差值确定偏差diff，确定小值b1=r+diff+c1和大值b2=r+diff+c2，记最大偏移量值为max，

当b2<0时，估计段始值为R临近的前一个段始值R1，估计偏移量范围是[b1+max，b2+max]，

当b1< 0<b2时，一个估计段始值为R临近的前一个段始值R1，估计偏移量范围是[b1+max，max]，另一个估计段始值为R，估计偏移量范围是[0，b2]，

当b1>max时，估计段始值为R临近的后一个段始值R2，估计偏移量范围是[b1-max，b2-max]，

当b1<max<b2时，一个估计段始值为R临近的后一个段始值R2，估计偏移量范围是[0，b2-max]，另一个估计段始值为R，估计偏移量范围是[b1，max]，

当b1和b2都不小于0，并且都不大于max时，估计段始值为R，估计偏移量范围是[b1，b2]；

若所述第一和第二动态变量由生成口令的次数确定，则以验证器保存的最近一次的第三动态变量增一后所确定的第二动态变量的第二段始值R和第二偏移量r为基础，根据系统确定的允许口令生成器连续生成口令，而这些口令又没有在验证器方成功使用的次数d，确定小值b1=r和大值b2=r+d，记最大偏移量值为max，

当b2>max时，一个估计段始值为R临近的后一个段始值R2，估计偏移量范围是[0，b2-max]，另一个估计段始值为R，估计偏移量范围是[b1，max]，

当b2不大于max时，估计段始值为R，估计偏移量范围是[b1，b2]。

21.如权利要求1-8之一所述的动态口令认证方法，其特征在于所述估计段始值和偏移量范围的方法是：

若所述第一和第二动态变量由时间确定，则以第二段始值R和第二偏移量r为基础，依据最近一次的第三动态变量与所述第二动态变量的差值确定应允许的误差范围[c1，c2]，依据最近一次的第三动态变量与最近一次的第二动态变量的差值确定偏差diff，再依据初次成功认证至最近一次成功认证指定时间间隔的数量d1计算平均偏差diff/d1，依据最近一次成功认证至当前认证指定时间间隔的数量d2估算一个偏差σ=（diff/d1）×d2，确定小值b1=r+diff+σ+c1和大值b2=r+diff+σ+c2，记最大偏移量值为max，

当 b2<0 时，估计段始值为R临近的前一个段始值R1，估计偏移量范围是[b1+max，b2+max]，

当b1< 0<b2时，一个估计段始值为R临近的前一个段始值R1，估计偏移量范围是[b1+max，max]，另一个估计段始值为R，估计偏移量范围是[0，b2]，

当b1>max时，估计段始值为R临近的后一个段始值R2，估计偏移量范围是[b1-max，b2-max]，

当 b1<max<b2 时，一个估计段始值为R临近的后一个段始值R2，估计偏移量范围是[0，b2-max]，另一个估计段始值为R，估计偏移量范围是[b1，max]，

当b1和b2都不小于0，并且都不大于max时，估计段始值为R，估计偏移量范围是[b1，b2]。

22.一种在由动态口令生成器与验证器构成的动态口令认证系统中使用的动态口令认证方法，动态口令生成器内有第一动态变量和第一秘密密钥，验证器内有第二动态变量和所述动态口令生成器的第二秘密密钥，所述动态口令生成器的第一动态变量和所述验证器的第二动态变量一致地、但独立地产生；其特征在于：

a） 要产生口令时，动态口令生成器的微处理器执行以下步骤：

a1） 根据预先给定的段长度和位置对第一动态变量进行分段，确定第一动态变量的第一段始值和第一偏移量，第一段始值为第一动态变量所在分段的起始位置，第一偏移量为该起始位置至第一动态变量的偏移；

a2） 由第一加密算法作用第一秘密密钥和第一段始值，得出第一动态密钥和第二动态密钥，第一动态密钥是第一加密算法输出结果的前半部分，第二动态密钥是第一加密算法输出结果的后半部分；用第一动态密钥产生第一动态变换表，根据第一动态变换表对第一偏移量进行变换，得出第一动态密码，该动态密码是第一动态变换表的输出结果；将第二动态密钥和第一偏移量结合生成第五动态密钥，再用第二加密算法作用第五动态密钥和第

一动态变量，得出第二动态密码，该动态密码是第二加密算法的输出结果；

a3）将第一动态密码和第二动态密码结合，生成动态口令；

b） 将该动态口令传送至验证器；

c） 要验证口令时，所述验证器的微处理器执行以下步骤：

c1）分离接收到的动态口令成第三动态密码和第四动态密码；根据预先给定的段长度和位置对第二动态变量进行分段，确定第二动态变量的第二段始值和第二偏移量，第二段始值为第二动态变量所在分段的起始位置，第二偏移量为该起始位置至第二动态变量的偏移；根据第二段始值和第二偏移量确定估计段始值和偏移量范围，估计段始值范围是以所述第二段始值为基础，选取第二段始值及其临近的段始值作为估计段始值，估计偏移量范围是以所述第二偏移量为基础，选取第二偏移量及其临近的偏移量作为估计偏移量；

c2）由第三加密算法作用第二秘密密钥和估计段始值，得出第三动态密钥和第四动态密钥，第三动态密钥是第三加密算法输出结果的前半部分，第四动态密钥是第三加密算法输出结果的后半部分；用第三动态密钥产生第二动态变换表，根据第二动态变换表对第三动态密码进行变换，得出第三偏移量，该偏移量是第二动态变换表的输出结果；

c3） 若第三偏移量在估计的偏移量范围内，则用第三偏移量和估计段始值还原出第三动态变量；将第四动态密钥和第三偏移量结合生成第六动态密钥，再用第四加密算法作用第六动态密钥和第三动态变量，得出验证码；将验证码与第四动态密码比较，若匹配并且该第三动态变量大于最近一次动态变量则用户合法，允许用户访问，验证过程结束；若不匹配或第三偏移量不在估计的偏移量范围内，则判断是否还有另外的估计段始值，若无则用户为非法，拒绝用户访问，验证过程结束；若有则取下一个估计段始值，转步骤c2）。

动态口令认证系统及方法

技术领域

本发明涉及通常的用口令(也称密码、通行字等)进行身份验证、访问控制的电子认证系统及方法。特别是涉及电子生成动态的、随机不可预测的口令，通过验证这些口令来正确识别已获得授权的个体或用户，并由此判定是否允许访问、进出、存取受保护的系统资源，是否提供有条件的服务，是否实现特许的业务往来等。本发明更特别地涉及各种通信网、电信网和计算机网中的访问控制和身份认证。

背景技术

口令是最广泛使用的一种验证用户身份合法性的方法。授权的用户都拥有一个区别于系统中其他用户的标识符 ID(用户名，序列码或帐号)和只有用户自己知道的秘密口令(PW 或 PIN)。如果用户想要登录系统，就须在请求节点键入自己的用户标识符和口令。系统内保留了所有授权用户的标识符和口令，认证节点利用收到的标识符提取该用户的正确口令，并用它与接收到的口令进行比较，如果匹配，则证明该用户身份合法，允许其进入系统或为其提供服务，否则该用户身份非法，拒绝其进入系统或不提供服务。在系统内直接保留用户的口令具有很大的风险，为了确保口令存放的安全性，一种解决方法就是用单向函数计算用户口令的杂凑值，并存储该值(例如 UNIX)。认证节点接收到用户的口令后，就用单向函数计算该口令的杂凑值，并与系统中正确的杂凑值比较，以确定其合法性。现在，随着通信网络化的迅猛发展，口令在网上来回传输的机会越来越多，传统的口令认证系统没有提供口令在网上传输的保护机制的问题日显突出，口令在网上被黑客截取的事件日益增多。为使口令安全传输，简单地将口令加密后在网上传送的办法是徒劳的，丝毫也不会提高安全性。因为，黑客同样可以截获这些密口令，无需还原密口令成明的形式，直接用截获的密口令来冒充授权用户，同样可以达到目的。密口令对认证节点来说只不过是多了一次脱密的程序，无法由此判定用户的真伪。

要彻底解决这个问题的办法就是使用动态的口令，使每个口令只一次有效，只在很短的时间内有效，使口令随时间不可预测地随机变化，致使黑客即使截获到口令也只是一个无用的失效口令。动态口令通常是借助于一个便于用户携带的，象信用卡大小的，或者外形象普通计算器一样的装置来生成，这里我们称它为动态口令生成器、口令生成器或生成器，也简称为卡(card)或者令牌(token)。

美国专利 US-4720860 揭示了一种动态口令认证系统，它应用一个静态变量和一个源于时间的动态变量作为保密的密码算法的输入参数。每位授权用户的动态口令生成器中存储有一个固定码，同时在该生成器的表面也印记了这个固定码，以防忘记。动态口令生成器每隔一个固定的时间间隔(例如每隔一分钟)就自动生成并显示一个不可预见的动态口令，它是该生成器将固定码作为静态变量输入进密码算法中，并以此时时钟的时间(当然也包括日期等在内，通常时间精细到分钟)作为动态变量输入进该算法后生成的。授权用户一旦要请求访问，就向认证节点传送自己的固定码和当时生成器所显示的动态口令。认证节点通过使用与生成器相同的密码算法，连同这个固定码和认证节点时钟的时间，原则上这个时间应与动态口令生成器所使用的时间相同，也生成一个动态口令，该口令与接收

到的口令相比较，以确定它们是否匹配。对于该系统，通过偷看授权用户所持有的口令生成器表面上印刻的符号，或在通信线路上截取，都可以很容易地获得固定码。因此，为了保证系统的安全性，计算口令的密码算法必须要保守秘密，如果算法的秘密被解开，整个系统的安全性都会因此而遭受损害。这也是为什么该专利要求，将密码算法存放在易挥发的存储器中，一旦企图解剖生成器，就彻底清除算法的原因。该专利中，无论是在授权用户持有的动态口令生成器方还是认证节点方的动态变量都要独立地生成，双方用来分别产生动态变量的时钟必须要一致，否则会拒绝正常的请求。但现实中，两个时钟之间有一定程度的相对偏差是不可避免的。在该专利的后续专利 US-4885778 中，揭示了一种保持时钟同步和具体验证用户的方法，它要求口令生成器在预先给定的时间间隔(例如 1 分钟，2 分钟等)生成口令，而认证节点方必须要用比用户口令生成器确定的时间间隔大得多的持续时间长度(例如 5 分钟，10 分钟等)来建立一个有效时间范围。当授权用户请求访问时，认证节点在有效的时间范围内计算多个口令(例如计算 5 个口令，10 个口令等)，如果用户的口令同其中之一匹配，则允许访问。显然，这个方法要求认证节点方的计算量要大得多，特别是，当口令生成器方同认证方的时钟偏差加大，所要求的有效时间长度相应地加大，认证节点方的计算量也随之明显地加大，因此，该方法必须要尽量缩短认证方有效时间长度才有较好的效果，这就对双方的时钟精度有较高的要求。另外，该方法不能较快速地排除接收到的非法口令，而且非法口令消耗系统的计算量要比任何合法口令所消耗的都多，因为，它必须要计算完有效时间内的所有口令，并逐一地同非法口令进行比较，到最后才能排除，这为黑客进行拒绝服务式攻击提供了便利。

在认证节点的服务器上可能具有较高精度、较稳定的时钟。但是，在口令生成器方情况就不一样了，降低制造口令生成器的生产成本是设计中要考虑的首要问题，在口令生成器上安装昂贵的、高质量和无偏差的时钟是不现实的。另外，口令生成器是提供给授权用户随身携带的，它的时钟容易受到许多不可预知的因素诸如温度变化、电压稳定性等的影响。因此，认证节点的时钟与口令生成器的时钟保持高度同步，在实际应用中是难以实现的，要同时与大量的口令生成器的时钟保持高度一致，则更是难以想象的。

试图在口令生成器上安装价格较低廉的时钟，使它与认证节点的时钟具有一定程度的同步就可达到生成安全可靠的动态口令一直是本领域努力的方向。美国专利 US-5887065 和 US-5937068(同一发明，分案申请)揭示了一种具有时钟同步的用户认证系统，它使用了一个源于时钟，另一个源于用户请求认证的次数(实际就是口令生成器生成动态口令的次数)两个动态变量。这两个变量结合在一起被一个随口令生成次数变化的密钥加密(密码算法可以是公知的，例如 DES，也可以是保密的)，加密后的结果或结果的一部分，与这两个变量的最低的一些有效比特位(例如 8 个比特，其中 4 个比特是当时时钟变量的最低 4 比特，另 4 个比特是生成口令次数变量的最低 4 比特)连接一起构成一个动态口令。在认证节点接收到口令后，用该口令中的同步信息替换认证节点方相应变量值的低有效比特位(例如分别替换两个变量的低 4 个比特)，判定替换后的变量是否在预先确定的有效范围以内，若不在其范围内，则对没有替换的高位部分增一或减一(例如在替换后的变量的第 5 比特位上加 1 或减 1)，再调节一次变量值，若都不在有效范围内，则认为该口令非法，拒绝访问；否则，只要在有效范围内，就用同一密码算法加密它们，并将加密的结果与用户的动态口令其余部分进行比较，匹配则认为该口令合法。在该认证系统中，由于其动态

口令中包含了一些明的同步信息，如果口令共有 n 个比特(例 n=30)，传递的同步信息为 m 个比特(例 m=8)，则该口令的真实长度只有 n-m 个比特(例 n-m = 22)。因为每次猜中该口令的概率是 $1/2^{n-m}=2^m \times 1/2^n$，也就是说，每次猜中该口令的概率比真正 n 比特口令的概率 $1/2^n$ 高出了 2^m 倍(例 256 倍)。在实际应用中，口令往往应当尽量的短，长口令会让用户厌烦，它既不实用，又不现实。因此口令中的每一比特位都十分珍贵，都应该充分地加以利用。在口令中以明的方式传递同步信息，也会降低生成动态口令的安全性，这些信息既为认证方的变量同步提供了便利，同时也为黑客和攻击者提供了重要信息。在生成口令时，这些信息既是密码算法的输入参数，又是决定密钥变化的参数，而且密码算法又是公开的，因此在知道了这些同步信息后，可以极大地缩小所要搜索的密钥空间。另外，决定口令生成的秘密密钥在每次生成口令之后都发生变化，会使认证节点对用户秘密密钥的管理带来不便，因为要安全有效地管理一个不断变化的秘密密钥会比管理一个固定的秘密密钥困难和复杂得多。

发明内容

本发明的目的就是要提供一个动态口令认证系统和方法，以改进以上的不足。特别地，本发明的目的就是要使每个动态口令生成器生成的动态口令都能够隐藏地传递同步信息给认证节点方，既为认证节点方提供有效的同步信息，又不降低生成动态口令的安全性；同时，认证节点方能够利用所恢复的该同步信息，较迅速地排除非法口令，提高验证口令的效率，另外，也降低了制作口令生成器的成本和实现难度。总之，就是要提供安全有效的动态口令认证的系统和方法。

本发明的目的通过以下技术方案实现：

本发明是一种在由动态口令生成器与验证器构成的动态口令认证系统中使用的动态口令认证方法，动态口令生成器内有第一动态变量和第一秘密密钥，验证器内有第二动态变量和所述动态口令生成器的第二秘密密钥，所述动态口令生成器的第一动态变量和所述验证器的第二动态变量一致地、但独立地产生；其特征在于：

a） 要产生口令时，动态口令生成器的微处理器执行以下步骤：

a1） 根据预先给定的段长度和位置对第一动态变量进行分段，确定第一动态变量的第一段始值和第一偏移量，第一段始值为第一动态变量所在分段的起始位置，第一偏移量为该起始位置至第一动态变量的偏移；

a2） 对第一秘密密钥、第一段始值、第一偏移量进行第一加密处理，得出第一动态密码，该动态密码是第一加密处理的输出结果；对第一秘密密钥、第一动态变量进行第二加密处理，得出第二动态密码，该动态密码是第二加密处理的输出结果；

a3） 将第一动态密码和第二动态密码结合，生成动态口令；

b） 将该动态口令传送至验证器；

c） 要验证口令时，所述验证器的微处理器执行以下步骤：

c1） 分离接收到的动态口令成第三动态密码和第四动态密码；根据预先给定的段长度和位置对第二动态变量进行分段，确定第二动态变量的第二段始值和第二偏移量，第二段始值为第二动态变量所在分段的起始位置，第二偏移量为该起始位置至第二动态变量的偏移；根据第二段始值和第二偏移量确定估计段始值和偏移量范围，估计段始值范围是以所述第二段始值为基础，选取第二段始值及其临近的段始值作为估计段始值，估计偏移量

范围是以所述第二偏移量为基础，选取第二偏移量及其临近的偏移量作为估计偏移量；

c2） 对第三动态密码、估计段始值和第二秘密密钥进行第三加密处理，得到第三偏移量，该偏移量是第三加密处理的输出结果；

c3） 若第三偏移量在估计的偏移量范围内，则用第三偏移量和估计段始值还原出第三动态变量，该动态变量是第三偏移量与估计段始值之和；对第二秘密密钥和第三动态变量进行第四加密处理，得到验证码，该验证码是第四加密处理的输出结果；将验证码与第四动态密码比较，若匹配并且该第三动态变量大于最近一次动态变量则用户合法，允许用户访问，验证过程结束；若不匹配或第三偏移量不在估计的偏移量范围内，则判断是否还有另外的估计段始值，若无则用户为非法，拒绝用户访问，验证过程结束；若有则取下一个估计段始值，转步骤c2）。

在所述步骤a2）中，对第一秘密密钥、第一动态变量和第一段始值进行第二加密处理，得出第二动态密码，该动态密码是第二加密处理的输出结果；相应地在所述步骤c3）中，对第二秘密密钥、第三动态变量和估计段始值进行第四加密处理，得到验证码，该验证码是第四加密处理的输出结果。

在所述步骤a2）中，对第一秘密密钥、第一动态变量、第一段始值和第一偏移量进行第二加密处理，得出第二动态密码，该动态密码是第二加密处理的输出结果；相应地在所述步骤c3）中，对第二秘密密钥、第三动态变量、估计段始值和第三偏移量进行第四加密处理，得到验证码，该验证码是第四加密处理的输出结果。

在所述步骤a2）中，第一加密处理包括第一加密算法和第一动态变换表，用第一加密算法作用第一秘密密钥和第一段始值，得出第一动态密钥，该动态密钥是第一加密算法的输出结果，用第一动态密钥产生第一动态变换表，再用第一动态变换表对第一偏移量进行变换，得出第一动态密码，该动态密码是第一动态变换表的输出结果；相应地在所述步骤c2）中，第三加密处理包括第三加密算法和第二动态变换表，用第三加密算法作用第二秘密密钥和估计段始值，得出第三动态密钥，该动态密钥是第三加密算法的输出结果，用第三动态密钥产生第二动态变换表，再用第二动态变换表对第三动态密码进行变换，得出第三偏移量，该偏移量是第二动态变换表的输出结果；

所述的用第一动态密钥产生第一动态变换表：$i \rightarrow S_i$ 的方法是，这里 $0 \le i < r$，$0 \le S_i < r$，正整数 $r=2^{m1}$，m1 是第一动态密码的比特数，先任意设定 S_i 初始状态，并将第一动态密钥按序填入 K_0，K_1，...K_{r-1} 中，可重复利用该密钥，直到填满整个 K_0，K_1，...K_{r-1}，执行下述动态置换表生成算法：先置 i 和 j 的值为 0，按序执行如下循环操作：a).先将 j 、S_i 和 K_i 的值相加，相加的结果被 r 除后所得的余数再作为 j 的值，b).然后对 S_j 和 S_i 彼此交换它们各自的值，c).最后将 i 的值增 1，若 i 小于 r 则返回该循环 a)步骤，否则退出该循环操作；由此得到该第一动态变换表：$i \rightarrow S_i$，其中 $0 \le i < r$，$0 \le S_i < r$；相应地所述的用第三动态密钥产生第二动态变换表：$i \rightarrow Q_i$ 的方法是，这里 $0 \le i < r$，$0 \le Q_i < r$，正整数 $r=2^{m1}$，m1 是第一动态密码的比特数，先按前述产生动态变换表步骤，在第三动态密钥作用下产生：$i \rightarrow S_i$，其中 $0 \le i < r$，$0 \le S_i < r$，再执行下述程序：先置 i 的值为 0，按序执行如下循环操作：a).先以 S_i 的值作为下标，将 i 的值作为 Q_{Si} 的值，b).然后将 i 的值增 1，若 i 小于 r 则返回该循环 a)步骤，否则退出该循环操作；由此得到该第二动态变换表：$i \rightarrow Q_i$，其中 $0 \le i < r$，$0 \le Q_i < r$。

所述的用第一动态密钥产生第一动态变换表得出第一动态密码的另一种方法是，由第一动态密钥生成的动态变换表：$i \rightarrow S_i$，这里 $0 \le i < r$，$0 \le S_i < r$，正整数 $r=2^{m1}$，m1 是第一动态密码的比特数，k 为第一偏移量，执行下述生成随机码组算法：先置 i 和 j 的值为 0，按序执行如下循环操作：a).先将 j 和 S_i 的值相加，相加的结果被 r 除后所得的余数再作为 j 的值，b).然后对 S_j 和 S_i 彼此交换它们各自的值，c).最后将 i 的值增 1，若 i 小于 k 则返回该循环 a)步骤，否则退出该循环操作；完成该循环操作后，就将 S_i 和 S_j 的值相加，相加的结果被 r 除后所得的余数为 t 值，取 S_t 的值为 K，由此得到的 K 作为第一动态密码；相应地所述的用第三动态密钥产生第二动态变换表得出第三偏移量的另一种方法是，以估计偏移量范围中的每个偏移量值作为 k，执行上述生成随机码组算法，得到相应结果 K，若 K 与第三动态密码匹配，则认为 k 就是所需的第三偏移量；

在所述步骤a2）中，第二加密处理包括第一加密算法和第二加密算法，用第一加密算法作用第一秘密密钥和第一段始值，得出第二动态密钥，该动态密钥是第一加密算法的输出结果，用第二加密算法作用第二动态密钥和第一动态变量，得出第二动态密码，该动态密码是第二加密算法的输出结果；相应地在所述步骤c3）中，第四加密处理包括第三加密算法和第四加密算法，用第三加密算法作用第二秘密密钥和估计段始值，得出第四动态密钥，该动态密钥是第三加密算法的输出结果，用第四加密算法作用第四动态密钥和第三动态变量，得出验证码，该验证码是第四加密算法的输出结果；

在所述步骤a2）中，第二加密处理包括第一加密算法和第二加密算法，用第一加密算法作用第一秘密密钥和第一段始值，得出第二动态密钥，该动态密钥是第一加密算法的输出结果，将第二动态密钥和第一偏移量结合生成第五动态密钥，再用第二加密算法作用第五动态密钥和第一动态变量，得出第二动态密码，该动态密码是第二加密算法的输出结果；相应地在所述步骤c3）中，第四加密处理包括第三加密算法和第四加密算法，用第三加密算法作用第二秘密密钥和估计段始值，得出第四动态密钥，该动态密钥是第三加密算法的输出结果，将第四动态密钥和第三偏移量结合生成第六动态密钥，再用第四加密算法作用第六动态密钥和第三动态变量，得出验证码，该验证码是第四加密算法的输出结果；

由第一和第三动态密钥产生的第一和第二动态变换表应大于所述的段长度。

所述第一和第二动态变量分段的方法是，根据预先确定一个段长度和位置，用段长度指定一段内含有多少个偏移量，确定最大偏移量，位置用来指定一段的起点，确定段始值。

所述第一和第二动态变量分别由动态口令生成器和验证器的时钟确定，或者由动态口令生成器已产生口令的次数确定。

若所述第一和第二动态变量由时间确定，则段长度应足以大于动态口令生成器的有效期内，其时钟与验证器时钟之间的最大可能偏差；

若所述第一和第二动态变量由生成口令的次数确定，则分段的长度应足以大于系统允许、没有由验证器验证、动态口令生成器连续生成的口令个数。

若所述第一和第二动态变量由时间确定，则动态变量应是有一个基本持续时间间隔的预先确定的时间单位的时间值或其函数值；

若所述第一和第二动态变量由生成口令的次数确定，则动态变量应是该次数值或其函数值。

用所述第一加密处理或第一加密算法作用第一段始值之前，对第一段始值进行第一编

码，该编码是第一段始值的表示形式，用所述第二加密处理或第二加密算法作用第一动态变量之前，对第一动态变量进行第二编码，该编码是第一动态变量的表示形式，所述第一编码和第二编码的方式是不同的；用所述第三加密处理或第三加密算法作用估计段始值之前，对估计段始值进行第三编码，该编码是第一段始值的表示形式，用所述第四加密处理或第四加密算法作用第三动态变量之前，对第三动态变量进行第四编码，该编码是第三动态变量的表示形式，所述第三编码和第四编码的方式是不同的。

当所述段长度不大于240时，取第一动态密码和第三动态密码的长度为8比特。

所述段长度的选取应使每天所确定的分段位置能够保持一致，位置的最佳选定应是用户较频繁地使用动态口令生成器时间值的最远点。

根据预先确定的段长度和位置，第一动态变量等于第一段始值与某个特定值之积并加上第一偏移量，第二动态变量等于第二段始值与某个特定值之积并加上第二偏移量，

在所述步骤c3）中，若所述的验证码与第四动态密码匹配，将所述第三动态变量与最近一次成功访问所还原的第三动态变量进行比较，若大于该值，则用户合法，允许用户访问，并用所述第三动态变量替代库中保存的最近一次成功访问所还原的第三动态变量，验证过程结束，若不大于该值，则用户非法，拒绝用户访问，验证过程结束。

所选取的估计段始值至少有一个，至多有两个。

所述估计段始值和偏移量范围的一种方法是：

若所述第一和第二动态变量由时间确定，则以第二段始值R和第二偏移量r为基础，依据最近一次的第三动态变量与所述第二动态变量的差值确定应允许的误差范围[c1，c2]，依据最近一次的第三动态变量与最近一次的第二动态变量的差值确定偏差diff，确定小值b1=r+diff+c1和大值b2=r+diff+c2，记最大偏移量值为max，

当b2<0时，估计段始值为R临近的前一个段始值R1，估计偏移量范围是[b1+max，b2+max]，

当b1< 0<b2时，一个估计段始值为R临近的前一个段始值R1，估计偏移量范围是[b1+max，max]，另一个估计段始值为R，估计偏移量范围是[0，b2]，

当b1>max时，估计段始值为R临近的后一个段始值R2，估计偏移量范围是[b1-max，b2-max]，

当b1<max<b2时，一个估计段始值为R临近的后一个段始值R2，估计偏移量范围是[0，b2-max]，另一个估计段始值为R，估计偏移量范围是[b1，max]，

当b1和b2都不小于0，并且都不大于max时，估计段始值为R，估计偏移量范围是[b1，b2]；

若所述第一和第二动态变量由生成口令的次数确定，则以验证器保存的最近一次的第三动态变量增一后所确定的第二动态变量的第二段始值R和第二偏移量r为基础，根据系统确定的允许口令生成器连续生成口令，而这些口令又没有在验证器方成功使用的次数d，确定小值b1=r和大值b2=r+d，记最大偏移量值为max，

当b2>max时，一个估计段始值为R临近的后一个段始值R2，估计偏移量范围是[0，b2-max]，另一个估计段始值为R，估计偏移量范围是[b1，max]，

当b2不大于max时，估计段始值为R，估计偏移量范围是[b1，b2]。

所述估计段始值和偏移量范围的另一种方法是：

若所述第一和第二动态变量由时间确定，则以第二段始值R和第二偏移量r为基础，依据最近一次的第三动态变量与所述第二动态变量的差值确定应允许的误差范围[c1，c2]，依据最近一次的第三动态变量与最近一次的第二动态变量的差值确定偏差diff，再依据初次成功认证至最近一次成功认证指定时间间隔的数量d1计算平均偏差diff/d1，依据最近一次成功认证至当前认证指定时间间隔的数量d2估算一个偏差σ=（diff/d1）×d2，确定小值b1=r+diff+σ+c1和大值b2=r+diff+σ+c2，记最大偏移量值为max，

当 b2<0 时，估计段始值为R临近的前一个段始值R1，估计偏移量范围是[b1+max，b2+max]，

当b1< 0<b2时，一个估计段始值为R临近的前一个段始值R1，估计偏移量范围是[b1+max，max]，另一个估计段始值为R，估计偏移量范围是[0，b2]，

当b1>max时，估计段始值为R临近的后一个段始值R2，估计偏移量范围是[b1-max，b2-max]，

当 b1<max<b2 时，一个估计段始值为R临近的后一个段始值R2，估计偏移量范围是[0，b2-max]，另一个估计段始值为R，估计偏移量范围是[b1，max]，

当b1和b2都不小于0，并且都不大于max时，估计段始值为R，估计偏移量范围是[b1，b2]。

本发明又是一种在由动态口令生成器与验证器构成的动态口令认证系统中使用的动态口令认证方法，动态口令生成器内有第一动态变量和第一秘密密钥，验证器内有第二动态变量和所述动态口令生成器的第二秘密密钥，所述动态口令生成器的第一动态变量和所述验证器的第二动态变量一致地、但独立地产生；其特征在于：

a） 要产生口令时，动态口令生成器的微处理器执行以下步骤：

a1） 根据预先给定的段长度和位置对第一动态变量进行分段，确定第一动态变量的第一段始值和第一偏移量，第一段始值为第一动态变量所在分段的起始位置，第一偏移量为该起始位置至第一动态变量的偏移；

a2） 由第一加密算法作用第一秘密密钥和第一段始值，得出第一动态密钥和第二动态密钥，第一动态密钥是第一加密算法输出结果的前半部分，第二动态密钥是第一加密算法输出结果的后半部分；用第一动态密钥产生第一动态变换表，根据第一动态变换表对第一偏移量进行变换，得出第一动态密码，该动态密码是第一动态变换表的输出结果；将第二动态密钥和第一偏移量结合生成第五动态密钥，再用第二加密算法作用第五动态密钥和第一动态变量，得出第二动态密码，该动态密码是第二加密算法的输出结果；

a3）将第一动态密码和第二动态密码结合，生成动态口令；

b） 将该动态口令传送至验证器；

c） 要验证口令时，所述验证器的微处理器执行以下步骤：

c1）分离接收到的动态口令成第三动态密码和第四动态密码；根据预先给定的段长度和位置对第二动态变量进行分段，确定第二动态变量的第二段始值和第二偏移量，第二段始值为第二动态变量所在分段的起始位置，第二偏移量为该起始位置至第二动态变量的偏移；根据第二段始值和第二偏移量确定估计段始值和偏移量范围，估计段始值范围是以所述第二段始值为基础，选取第二段始值及其临近的段始值作为估计段始值，估计偏移量范围是以所述第二偏移量为基础，选取第二偏移量及其临近的偏移量作为估计偏移量；

c2）由第三加密算法作用第二秘密密钥和估计段始值，得出第三动态密钥和第四动态密钥，第三动态密钥是第三加密算法输出结果的前半部分，第四动态密钥是第三加密算法输出结果的后半部分；用第三动态密钥产生第二动态变换表，根据第二动态变换表对第三动态密码进行变换，得出第三偏移量，该偏移量是第二动态变换表的输出结果；

c3）若第三偏移量在估计的偏移量范围内，则用第三偏移量和估计段始值还原出第三动态变量；将第四动态密钥和第三偏移量结合生成第六动态密钥，再用第四加密算法作用第六动态密钥和第三动态变量，得出验证码；将验证码与第四动态密码比较，若匹配并且该第三动态变量大于最近一次动态变量则用户合法，允许用户访问，验证过程结束；若不匹配或第三偏移量不在估计的偏移量范围内，则判断是否还有另外的估计段始值，若无则用户为非法，拒绝用户访问，验证过程结束；若有则取下一个估计段始值，转步骤 c2）。

本发明对动态变量实施分段策略，来解决口令生成器的动态变量与验证器方动态变量的同步问题。预先确定一个分段长度 L 和位置，分段长度 L 指定一段内含有多少个偏移量，即确定了偏移量的取值；位置指定一段的起点，即确定了段始值的选取。在分段长度 L 和分段位置确定的前提下，任意个动态变量即可唯一地确定一个段始值和一个偏移量，反之，由一个段始值和一个偏移量也可唯一地确定一个动态变量。实际上，任意动态变量都可以看成是其所确定的段始值与所确定的偏移量的一种组合。

如果动态变量由时间确定，为动态变量分段的长度 L 应当足以大于在动态口令生成器的有效期内，其时钟与验证器时钟之间的最大可能偏差。这致使验证器估计口令生成器的段始值至多不会超过两个。验证器方是依据自己的时钟来估计段始值和相应偏移量的范围。如果动态变量由生成口令的次数确定，为动态变量分段的长度 L 应足以大于系统允许没有由验证器验证的、口令生成器连续生成的口令次数。验证器方是依据对该用户最近一次的成功验证所还原的动态变量增一后，来估计段始值和相应偏移量的范围。

本发明的优点是：

1.由于本发明引入分段策略来处理动态变量，无需要求双方所产生的动态变量保持非常一致，仅需由双方的动态变量所确定的段始值能相对同步，使动态口令生成器上的动态变量与验证器方的动态变量之间的偏差小于最大偏移量值就可以达到正确验证动态口令的目的，这有效地解决了口令生成器方的动态变量与验证器方的动态变量之间的同步问题，这既为动态口令认证的实现提供了便利，也为降低制作口令生成器的成本创造了条件。通常情况下，验证器方仅需要估计一个段始值就够了，只有当口令生成器的动态变量所确定的偏移量接近其可能的最小值或最大值时，才会出现需要估计两个段始值的情况。另外，通过利用接收到的动态口令中的第一个动态密码所还原出的值，就可以排除掉绝大多数的非法口令，从而实现了较迅速地排除非法口令的访问，提高了验证口令的效率。

2.由于本发明利用动态变量的段始值在秘密密钥和第一个算法的作用下，生成两个随机的、不可预见的动态密钥。其中，第一个随机、不可预见的动态密钥确定出一个随机、不可预见的动态变换表，由该变换表将偏移量替换为随机、不可预见的第一个动态密码；这样就达到了隐藏地给验证器方传递同步信息的目的，使得用户所用动态口令的每一个比特既安全又有效，消除了传递多余明同步信息所造成的诸多不利。另外，第二个随机、不可预见的动态密钥与动态变量在第二个算法的作用下生成第二个随机、不可预见的动态密

码；或者是先将第二个动态密钥与偏移量结合生成另一个随机、不可预见的动态密钥，再将该动态密钥与动态变量在第二个算法的作用下生成第二个随机、不可预见的动态密码，这样就实现了由不断变化的密钥来决定第二个动态密码的生成，同时实现了由不断变化的密钥来决定由第一动态密码和第二动态密码构成的动态口令的生成，并使验证器方无需管理一个不断变化的密钥，仅需管理决定该动态密钥的固定不变的密钥。

附图说明

下面结合附图对本发明作详细描述。

图 1 是口令认证系统的一般性简图；

图 2 是本发明两个动态口令生成器的正面视图；

图 3 是本发明举例说明对动态变量分段的实例；

图 4 是本发明的动态口令生成器生成动态口令时的操作运行原理流程图；

图 5 是本发明的验证器验证接收到的动态口令时的操作运行原理流程图；

图 6 是本发明的动态变量由时间确定时，验证器估计段始值及其相应偏移量范围的流程图；

图 7 是本发明的动态变量由动态口令生成器生成口令的次数确定时，验证器估计段始值及其相应偏移量范围的流程图；

图 8 是本发明的动态口令生成器生成动态口令和验证器验证接收到的动态口令时的简明流程图。

发明具体实施方式

本发明的系统包括至少一个(通常是许多)由授权用户持有的动态口令生成器和至少一个(可以有多个)能接收授权用户的口令并能据此判定用户合法性的验证器。

本发明的口令生成器内部至少包括能执行本发明方法的动态口令生成程序的普通微处理器和能存储该程序和口令生成器密钥的存储器，需要时也拥有自己的电源，以提供运行程序的能量；对于生成与时间相关口令的口令生成器还需要有一个能提供时间信息的时钟。口令生成器通常是便于携带的、小巧的、其形状和大小如同信用卡或计算器；图 2 是两个口令生成器的正面视图，它们都有一个显示屏 201，以显示所生成的口令或其它相关信息；当然，显示屏 201 也可以使用发声装置来代替，即不使用显示，而使用声音；200 是仅有开关触发键 202 的口令生成器，这主要用于仅支持一个验证器或生成与时间相关的口令，并且口令生成器无需用 PIN 保护的情形，该种生成器的操作极为方便，当按一下触发键 202，口令生成器根据预先确定的时间单位所具有的持续时间间隔不断地生成并在显示屏 201 上显示所生成的动态口令，授权用户就用当时显示的口令传递给验证器方，当再按一下该键 202，就能终止口令的生成和显示，如此循环往复。图 2 的另一种口令生成器 203 有多个按键 204，如数字键或功能键等，这主要用于能同时支持多个独立的验证器，或者口令生成器需用 PIN 保护，以防止口令生成器丢失后被非授权人员滥用的情形，该种生成器具有更好的保护措施，在生成口令之前，授权用户须先输入自己的 PIN，只有当输入的 PIN 与存储在口令生成器中的 PIN 相同时，口令生成器才能启动口令生成程序。对于生成与时间无关的动态口令生成器，还可以用普通的智能卡实现，这可以省却电源，省却按键和显示屏，而利用读卡终端或相连接计算机上的按键和显示屏，这种生成器可大幅降低制造生成器的成本，可广泛应用于带读卡终端的环境里。

图 1 是本发明的动态口令认证系统的一般性简图。图中的 100 是授权用户才持有的口令生成器，请求节点 101 是授权用户向验证器 103 传递自己的用户 ID 和口令的工具，101 可以是计算机、客户端、电话、手机等。请求节点也可以与口令生成器合二为一，例如将口令生成器做成固件嵌入于计算机等各种通信设备中，或者软件形式的动态口令生成器。通信通道 102 可由已知的任意类型的通信方式构成。验证器 103 包括能执行本发明方法的动态口令验证程序的处理器，以及能存储该程序和授权用户有关信息的存储器。验证器 103 在认证节点 104 内，认证节点 104 可以是主机、服务器，也可以是作为访问控制服务器的专用计算机；验证器 103 的口令验证程序可作为服务器程序驻留于认证节点 104 中，例如作为守护程序，并使用认证节点的 CPU 和时钟资源等，因此，可以将认证节点与验证器等同起来。当验证器 103 接收到从请求节点 101 传来的用户 ID 和动态口令，口令验证程序就将验证该动态口令，并确定该用户口令的正确性，若口令正确，则认为该用户是授权的合法用户，系统允许其访问资源或获得有条件的服务 105 等，若口令不正确，则认为该用户是非法的，就拒绝该用户访问。

动态口令生成器能生成动态口令是因为口令生成器内的动态变量能不断变化，验证器生成的口令与口令生成器生成的口令能够一致，则是因为验证器方能够确定口令生成器方生成口令的动态变量。本发明的动态变量的一种情况是由时钟产生的日期和时刻所确定(以下简称由时间确定)，它生成与时间相关的口令；动态变量另一种情况是由口令生成器产生口令的次数所确定，它生成与时间无关的口令。

如果动态变量由时间确定，动态变量应是预先确定的精细程度(或称时间单位)的时间值或其函数值(例如，动态变量可以是时间值与某个特定数之积或之和后的值)，这个精细程度或时间单位有一个基本的持续时间间隔，该时间间隔决定了口令多长时间就要发生变化，例如时间单位为 15 秒、30 秒、1 分钟等，则动态口令生成器每隔 15 秒、30 秒、1 分钟等所产生的口令就会发生变化；例如，若生成口令时的时间是 2000 年 1 月 30 日 9 点 35 分 0 秒钟或者 59 秒钟，当时间单位是 1 分钟时，以 0 秒为该基本持续时间间隔的起点，无论是 0 秒钟还是 59 秒钟，动态变量都取 2000 年 1 月 31 日 9 点 35 分(当然，也可以取其它某秒为基本持续时间间隔的起点，这种情况不再赘述)；当时间单位是 30 秒，0 秒钟时的动态变量取 2000 年 1 月 31 日 9 点 35 分，而 59 秒钟时的动态变量取 2000 年 1 月 31 日 9 点 35 分 30 秒。

如果动态变量由口令生成器生成口令的次数确定，动态变量就是该次数值或其函数值(例如，动态变量可以是该次数值与某个特定数之积或之和后的值)，口令生成器在生成一次口令后，该动态变量自动增一。例如口令生成器已产生了 1000 个口令，则此时产生口令的动态变量就是 1000，产生下一次口令的动态变量则变为 1001。

本发明对动态变量实施了分段策略，有效地解决了口令生成器的动态变量与验证器方动态变量的同步问题。预先确定一个分段长度 L 和位置选取，分段长度 L 指定一段内含有多少个偏移量，即偏移量最小可能值为 0，最大可能值为 L-1；位置指定一段的起点，即确定段始值的选取。由此，任意个动态变量就可唯一地确定一个段始值和一个偏移量，反之，由一个段始值和一个偏移量也唯一地确定一个动态变量。实际上，任意动态变量都可以看成是其所确定的段始值与所确定的偏移量的一种组合，例如它们之和，或更一般地，将动态变量表示成其所确定的段始值与某个特定值之积并加上所确定的偏移量，例如这个

特定值可为预先确定的一个整数。对动态变量分段的长度L和位置的确定可以在一个认证系统内统一确定(即该系统内所有口令生成器的L和位置的选取都是一样的)，也可以针对每一个口令生成器设置其L和位置的选取，甚至，也可以将它们的选取作为口令生成器可调节的参数，根据使用情况进行调节，当然，这个调节需要告知验证器方，验证器方也做相应的变化。

若动态变量由时间确定，分段的长度L应当足以大于该动态口令生成器在有效期内，其时钟与验证器时钟之间的最大可能偏差，或系统内所有口令生成器的时钟与验证器的时钟之间的最大可能偏差(系统统一确定情形)，例如估计一个口令生成器的时钟与验证器的时钟的偏差最大可能值为60分钟，则当时间单位选取的是1分钟时，L至少应为60，当时间单位选取的是30秒时，L至少应为120。若系统内所有口令生成器的时钟与验证器的时钟的偏差最大可能值为两个小时，则系统可统一确定的L至少为120（当时间单位是1分钟）或L至少为240（当时间单位是30秒）。分段位置的选定最好避开用户较频繁地使用口令生成器的时间，假如上午9点左右用户使用较为频繁，L=120（时间单位是1分钟），则位置可选取为每天的8、10、12、14、16、18、20、22、0、2、4、6点整。这致使在该频繁期里，验证器估计口令生成器的段始值只会有一个(只有偏移量太大或太小时，才会出现需估计两个段始值的情况)，由此，更有效地验证用户的口令。另外，为便于确定段始值和偏移量，分段长度L的选取最好使每天所确定的分段位置能够保持一致，例如，若选取的位置是8、10、12、14、16、18、20、22、0、2、4、6点整，则每天均能以此循环。假定口令生成器的有效使用期是四年，这里给出L和位置选取的具体实例：

基本时间单位	L	每个月的平均偏差	位置选定
15秒	120	〈 37.5秒	每天的0.5、1、1.5、...、23.5、0点
15秒	240	〈 75秒	每天的0、1、2、3、...、22、23点
30秒	120	〈 75秒	每天的0、1、2、3、...、22、23点
1分	60	〈 75秒	每天的0、1、2、3、...、22、23点
1分	120	〈150秒	每天的0、2、4、6、...、20、22点
1分	180	〈225秒	每天的0、3、6、9、...、18、21点
1分	240	〈300秒	每天的0、4、8、12、16、20点

基本时间单位就是前面所指的决定动态变量的时间单位，也是一个动态口令持续的时间，超过该持续时间，口令就会发生变化；所估计的口令生成器时钟与验证器所用时钟之间平均每个月的偏差应当足以小于上面的值；口令生成器时钟与验证器所用时钟之间的偏差越小，所使用的基本时间单位就可以越短，一个动态口令持续的时间越短，系统提供的安全性就越高。从上面的结果可以看出，通常将L限制在240以内，就可以满足大多数实际应用的需要。

若动态变量由生成口令的次数确定，则分段的长度L应足以大于系统允许没有由验证器验证的、口令生成器连续生成的口令次数，例如设L=32，则用户使用口令生成器产生口令时，不能连续生成32个没有成功使用的口令，也就是说，这连续的32个口令必须有一个在验证器方获得验证，否则就会失去同步。由于此种动态变量对用户使用口令生成器的敏感性，最好使用有PIN保护的口令生成器，即图2的203有多个按键204的口令生成器。这可以有效地制止该情况的发生。

图 3 的 300 是对时间动态变量分段的一个例子，如果动态变量的时间单位是 1 分钟，L=120，即每段内有 120 个动态变量，位置取的是每天的 0、2、4、6、8、10、12、14、16、18、20、22 点整，302 是 8 点 31 分(为叙述方便，将日期缺省，后面的例子均如此处理)，305 是 8 点 31 分 50 秒，则它们的段始值为 8 点整（301 为 8 点整，是 302 和 305 所在分段的起始位置），偏移量都为 31；304 是 10 点 13 分 12 秒，则其段始值为 10 点整（303 为 10 点整，是 304 所在分段的起始位置），偏移量为 13。如果动态变量的时间单位是 30 秒，L=240，位置取的仍然是每天的 0、2、4、6、8、10、12、14、16、18、20、22 点整等，302 的段始值为 8 点整，偏移量为 62；305 的段始值为 8 点整，偏移量为 63；304 的段始值为 10 点整，偏移量为 26。

图 3 的 310 是对次数动态变量分段的一个例子，这里 L=32，位置取的是 0、32、64、96...等，312 是 18，则其段始值为 0（311 为 0，是 312 所在分段的起始位置），偏移量为 18；314 是 37，则其段始值为 32（313 为 32，是 314 所在分段的起始位置），偏移量为 5；315 是 64，则其段始值为 64，偏移量为 0。

图 4 是当用户触发动态口令生成器，如按一下图 2 的 202 键或 204 的某键等，口令生成器执行各种操作，以产生动态口令时的简明流程图。

对于有 PIN 保护或支持多个验证器的口令生成器图 2 的 203，授权用户经 204 输入只有自己知道的 PIN 401，口令生成器在 402 判别该 PIN 正确与否，例如生成器中保存有正确的 PIN，将 PIN 401 与此比较，判定 PIN 401 的正确性；如果不正确，在 403 拒绝进一步执行，关闭生成器。如果正确，若支持多个验证器，还要求 204 输入请求访问的验证器代码 404，这样就启动了生成口令的程序(对图 2 的 200，仅需按一下 202 就启动口令生成程序)。口令生成器先确定此时的动态变量 406，若动态变量 406 由时间确定，则从时钟取时间，若动态变量 406 由生成口令的次数确定，则从存储该参数的存储器中取该动态变量，并根据已确定的 L 和位置确定该动态变量的段始值 407 和偏移量 411。段始值 407 和动态变量 406 可用不同的表示形式，来作为编码 408 和编码 412 的输入值，也可以认为将段始值 407 和动态变量 406 用不同的表示形式，作为编码 408 和编码 412 的开始。例如对于时间确定的动态变量 406，编码 412 可用相对于一个指定起始点(例如 2000 年 1 月 1 日 0 点)至此时(例如 2000 年 1 月 1 日 8 点 31 分)的时间单位(例如 1 分钟)的个数来确定(例如 511 整数值)，编码 408 可直接使用该时间的字符串表示，如段始值为 2000 年 1 月 1 日 8 点，可用“2000010108”的 ASCII 码表示；对于口令生成次数确定的动态变量(例如次数为 131)，编码 412 可用该次数的整数值(例如 131 的整数值)，编码 408 也可用字符串表示，如段始值为 128，可由“128”的 ASCII 码表示。编码 408 和编码 412 对如上表示的值进行填补、取舍或进行一些简单的运算使其输出符合算法 410 和算法 417 的输入要求，并使它们的区别加大。对于支持多个验证器的情形，验证器代码需同段始值连接在一起作为编码 408 的输入。另外，PIN 是否同验证器代码一起作为编码 408 的输入可以设定为系统可选方案，若 PIN 也作为编码 408 的输入，验证器方也需要存储该用户的 PIN，由此构成一种双因素验证方案，即验证器不仅需要该口令验证器的秘密密钥，也需要用户的 PIN。

算法 410 和算法 417 可以是公开的密码算法，也可以是保密的算法；算法 410 和算法 417 可以是相同的，也可以有一些区别；这两个算法都应当是密码学意义上安全的密码算法，例如加密算法 DES，单向杂凑算法 SHA 等，也可以是密码学意义上安全的伪随机数

发生器 PRNG，例如 ANSI X9.17 标准，FIPS 186 标准等所建议的生成伪随机数的方法等。无论使用哪一种算法或方法，其目的都是使算法 410 和算法 417 输出的结果具有很好的随机性和不可预见性，至于具体使用哪一个算法或方法，并不是本发明的主要内容，因此这里将可逆的加密算法、单向的杂凑算法或其它的密码算法以及它们的组合等统称为加密处理(如所述的加密处理-1、加密处理-2、加密处理-1a、加密处理-2a 等)。为了举例说明的方便，这里假定算法 410 和 417 都是单向杂凑算法 SHA。

动态口令生成器的秘密密钥 405 和编码 408 的输出作为算法 410 的输入，在 SHA 作用后输出 160 比特的结果，取前 80 比特作为第一个动态密钥 413，取后 80 比特作为第二个动态密钥 414。第二个动态密钥 414 和编码 412 的输出作为算法 417 的输入，在 SHA 作用后输出 160 比特的结果，根据事先已确定生成动态口令 421 的长度 m1+m2 比特，其中第一个动态密码为 m1 比特，第二个动态密码为 m2 比特(为叙述方便，以下均以二进制为例进行说明，对于十进制、十六进制等同样可以类似地说明，不再赘述)，取算法 417 输出结果的前面 m2 个比特(当然也可以取其它位置的 m2 比特)作为第二个动态密码 420。本发明的一种简单方法是以秘密密钥 405 或其一部分作为算法 417 的密钥，作为编码 412 的输入后生成第二个动态密码 420。本发明的另一种较好的情况是，第二个动态密钥 414 先与偏移量 411 在 415 结合，生成一个新的动态密钥 416，再以这个新的动态密钥 416 作为密钥与编码 412 的输出作为算法 417 的输入。这里在 415 的结合可以是各种逻辑或算术运算如模二加等，更安全的是使用一次单向杂凑函数，例如以第二个动态密钥 414 和偏移量 411 输入进 SHA，其输出的结果作为新的动态密钥 416，因此该结合的选择余地是非常大的，只要使其输出具有较好的随机性和不可预见性。由于在 415 的结合作用下，使每一次生成第二个动态密码 420 所使用的密钥都不一样。根据第一个动态密钥 413，生成一个能替代所有偏移量的动态变换表 418，由该变换表将偏移量 411 变换成一个 m1 比特的第一个动态密码 419。

一种生成动态变换表 418 的方法是在第一个动态密钥 413 的作用下，生成长度为 r(r 等于 2 的 m1 次幂，如 m1=8 时，r =256）的动态置换表：

$$i \rightarrow S_i \qquad (0 \le i < r,\ 0 \le S_i < r)。$$

这样，偏移量为 k 时，第一个动态密码 419 就是 S_k。由随机、不可预测的第一个动态密钥 413，创建一个随机、不可预测的置换表是不困难的，效率也是非常高的。这里可按如下步骤生成：

首先，设定 S_i 的初始状态。可以设定为明的、任意确定的一个初始状态，例如取 S_0= r -1，S_1=r-2，...，S_{r-2}=1，S_{r-1}=0，也可以将 S_i 的初始状态作为口令生成器的密钥，即每个口令生成器的 S_i 的初始状态都是不一样的，保密的。

然后，将第一个动态密钥 413 按序填入 K_0，K_1，...K_{r-1} 中（每个 K_i 均为 m1 个比特），如果第一个动态密钥 413 不够长，可重复利用该密钥，直到填满整个 K_0，K_1，...K_{r-1}，执行下述程序：

```
        j  〈== 0;
FOR  i  FROM 0 TO r-1  DO
   BEGIN
        j  〈==  (j + Si + Ki)   MOD r;
```

```
        R ⟨== Sj;
        Sj ⟨== Si;
        Si ⟨== R;
    END
```

由此，就可以得到由动态密钥 413 决定的一个动态置换表：

$i \rightarrow S_i$ （$0 \le i < r$，$0 \le S_i < r$）。

m1 的取值应不小于最大偏移量所拥有的比特数，通常取 r 适当地大于最大偏移量值。这样，由置换表的随机、不可预测性，可以提高第一个动态密码 419 的随机、不可预测性。这里以最坏的情况进行分析，设 L 是分段长度，r 等于 2 的 m1 次幂，在偏移量为 0 时，猜中其对应的第一个动态密码 419 的概率是 1/r；偏移量为 1 时，假定已知道偏移量为 0 时的结果，猜中对应第一个动态密码 419 的概率是 1/(r-1)，....；偏移量为 L-1 时，假定已知道前面所有结果，猜中对应的第一个动态密码 419 的概率是 1/(r-L+1)；对任意一个偏移量，猜中对应的第一个动态密码 419 的平均概率 P=(1/r + 1/(r-1)+ ... +1/(r-L+1))/L，当 r 越大于 L，该平均概率 P 就越小，因此，适当选取比 L 大一些的 r 即可满足实际的需求。例如下面几种情况：

m1	L	平均概率 P
8	60	0.4441%
8	120	0.5257%
8	180	0.6721%
8	240	1.1432%
9	240	0.2632%

可见，当 L = 60，120 或 180，m1 = 8 时，猜中对应的第一个动态密码 419 的平均概率 P 是远远小于 1/128 = 0.7812%，后者是猜中 7 个比特完全随机、不可预测码的概率，因此，这里使用长度为 256 的随机置换表所替代的 8 个比特的第一个动态密码 419 被猜中的概率远远要小于猜中 7 个比特完全随机、不可预测码的概率 1/128；对于 L=240，m1=8 时的平均概率 P 也远远小于 1/64 =1.5625%，后者是猜中 6 个比特完全随机、不可预测码的概率；对于 L=240，m1=9 时的平均概率 P 要远远小于 1/256 = 0.3906%，后者是猜中 8 个比特完全随机、不可预测码的概率。

另一种生成动态变换表 418 的方法是在第一个动态密钥 413 的作用下，生成共 L 组随机不可预测码，其中每组均为 m1 个比特，为叙述方便不妨称为生成随机码组方法。当偏移量 411 为 k 时，则取第 k 组随机不可预测码作为第一个动态密码 419。具体可按如下步骤生成：

首先，按照上述方法生成一个动态置换表：$i \rightarrow S_i$ （$0 \le i < r$，$0 \le S_i < r$）。

然后执行如下程序：

```
        j ⟨== 0;
    FOR i FROM 0 TO k DO
      BEGIN
        j ⟨== (j + Si) MOD r;
        R ⟨== Sj;
```

S_j 〈== S_i;

S_i 〈== R;

END

t 〈== (S_i+S_j) MOD r;

K 〈== S_t;

这里，k 是图 4 的偏移量 411 的值，K 就是所求的第 k 组随机、不可预测码，即以此作为第一个动态密码 419。按该种方法生成的 m1 个比特的第一个动态密码 419 被猜中的概率均为 $1/2^{m1}$。

这样一来，我们就达到了隐藏地传递同步因子的目的，使用较少随机、不可预测的比特码既传递了同步信息，又使口令的每个比特安全可靠，从而克服了 US-5887065 以明的形式传递同步信息的种种弊端。

最后，将第一个动态密码 419 与第二个动态密码 420 结合在一起就构成了所要生成的动态口令 421，例如，将第一个动态密码 419 与第二个动态密码 420 简单地连接在一起构成动态口令 421，或者将第一个动态密码 419 的每一个比特按照预先指定的位置插入进第二个动态密码 420 之中构成动态口令 421 等，都是具体的结合方式，这个结合应当是可以分离的，即依据该结合方式，验证器方可从图 5 的动态口令 421a 分离出动态密码 419a 和动态密码 420a。由于第一个动态密码 419 与第二个动态密码 420 是完全无关的随机、不可预测码，因此猜中动态口令 421 的概率是猜中第一个动态密码 419 的概率与猜中第二个动态密码 420 的概率之积。对于由生成口令次数确定的动态变量，在生成动态口令 421 之后，还需将存储在口令生成器的存储器中的该动态变量自动增一。

图 5 是验证器在获得用户的请求和口令后，为验证该动态口令，验证器操作运行原理的简明流程图。验证器拥有一个信息库 501，它包含授权用户信息或口令生成器的秘密密钥，以及验证器每次验证后所记录的、用于同步口令生成器动态变量的有关信息。验证器接收到用户 ID 506(或用生成器的序列号替代用户 ID，以下均假设为用户 ID)和动态口令 421a 后，如果是基于时间的动态口令，还需根据验证器的时钟，记录下接收到该动态口令的时间。依据用户 ID 506 从信息库 501 中提取该口令生成器的秘密密钥 405a，并利用信息库中所记录的该口令生成器的信息，在 502 估计该口令生成器生成动态口令的段始值及偏移量的范围，其具体估计方法在后面专门描述。在 407a 取一个估计的段始值，如果是支持多个验证器或者 PIN 也要发生作用，还要从信息库 501 中取验证器代码 404a 或 PIN，经编码 408a(编码 408a 应与编码 408 一致，这里将与图 4 中功能一致或相近的方框均以附加 a 来表示，例如 408a 与 408，也将验证器方与生成器方对应的各功能附加 a 来表示，例如加密处理-1 与加密处理-1a 等)，秘密密钥 405a 与编码 408a 的输出作为算法 410a 的输入参数，输出动态密钥 413a 和动态密钥 414a。根据动态密钥 413a 生成动态变换表 418a，要生成与前述动态变换表 418 的对应变换表的具体方法是，先按前述生成动态置换表的步骤，在动态密钥 413a 的作用下生成置换表 i → S_i ($0 \le i < r$，$0 \le S_i < r$)，再按如下程序即得其逆置换：

FOR i FROM 0 TO r-1 DO

BEGIN

J 〈== S_i;

Q_j 〈== i;

END

由此得到逆置换表：i → Q_i （0≤i<r，0≤Q_i<r）。将从动态口令 421a 分离的动态密码 419a（如为 i）经变换表 418a 变换，生成所需偏移量 411a（如为 Q_i），在 503 判断还原的偏移量 411a 是否在估计的偏移量范围内，如果偏移量 411a 在该范围内，则在 406a 依据此时在 407a 取得的段始值和偏移量 411a 还原出一个动态变量；如果偏移量 411a 不在该范围内，则执行步骤 504。

对应于另一种生成动态变换表 418 的方法，是以在 502 中估计的偏移量范围中的每个偏移量值作为 k，执行前面描述的生成随机码组的方法，得到相应结果 K，若 K 与动态密码 419a 匹配，则认为 k 就是所需的偏移量 411a，并在 406a 依据此时在 407a 取得的段始值和偏移量 411a 还原出一个动态变量；若在估计的偏移量范围内都没有匹配的结果，则执行步骤 504。

在 504 询问是否还有其它估计的段始值(最多只可能有两个段始值)，若还有，则返回至 407a 取下一个估计段始值再进行上述过程。如果没有其它估计段始值了，则在 505 拒绝访问，判定该口令不正确，不是授权用户。在这里，绝大部分的非法口令都会被排除掉，而无需再进行后面进一步的操作，因此，较好地解决了 US-4885778 中所存在的，不能有效排除非法口令的问题。下表是各种条件下，排除非法口令的概率，这里设第一动态密码 419 的长度为 8 个比特，即 m1 = 8：

所估计偏移量范围内偏移量的个数	排除非法口令的平均概率
1	99.609%
2	99.219%
3	98.828%
4	98.437%
5	98.047%
6	97.656%
7	97.266%
8	96.875%
9	96.484%
10	96.094%

因此，只要 L<256，设定第一个动态密码 419 的长度为 8 个比特是较理想的。因为，价格低廉而流行的单片机是 8 位机，运行上述生成动态变换表的程序的效率会非常高，因此选择 8 个比特的第一个动态密码 419 无论在安全需求、运行效率、空间大小等各方面都是较好的一个折衷。当然根据特定的需要，实际地加长或缩小第一个动态密码 419 的比特数也是可以的。例如，增加一个比特，在同样条件下，排除非法口令的平均概率就会进一步地提高。

在 406a 依据在 407a 所取的估计段始值和偏移量 411a 还原出一个动态变量，例如用该段始值与偏移量 411a 之和还原出一个动态变量，在 406a 还原出的动态变量经编码 412a 后和动态密钥 414a 同时作为算法 417a 的输入参数。另一种情况是，动态密钥 414a 先与偏移量 411a 在 415a 结合后生成一个新的动态密钥 416a，然后再与编码 412a 的输出一起

同时作为算法 417a 的输入参数。算法 417a 的输出或输出的一部分作为验证码 420b，验证码 420b 与从动态口令 421a 中分离出的动态密码 420a 在 511 进行比较，如果不匹配，则返回至 504 进行上面所述的操作。如果匹配，则在 507 判断在 406a 还原的动态变量是否大于信息库 501 中记录的该口令生成器最近一次成功访问所用的动态变量(简称最近一次动态变量)，如果不大于此，在 505 拒绝访问，这就彻底杜绝了重放攻击；如果大于此，则验证器认为该口令是合法的，该用户是授权用户，在 509 允许其访问系统资源或提供指定服务等，同时，在 510 将 406a 步骤中所还原的动态变量用来替代信息库中存储的最近一次动态变量，作为新的最近一次动态变量。另外，如果是基于时间的动态变量，在 510 还要将在 406a 还原的动态变量与验证器接收到该动态口令时所记录的时间所确定的动态变量(图 6 的 601 步骤所确定的 T)之间的差值作为偏差 diff，存入信息库中，以替代原有的偏差。

图 8 所示口令生成和口令验证时的流程图是图 4 和图 5 的几种替代方案，算法 417 的输入密钥可以有三种方式，第一种是用秘密密钥 405 或其中一部分直接作为算法 417 的密钥，第二种是秘密密钥 405 同段始值 407 进行运算（例如用 SHA 算法作用，即它们同时作为 SHA 算法的输入参数）后，取其输出或其输出的一部分作为算法 417 的密钥，第三种是由秘密密钥 405 同段始值 407 进行运算（例如用 SHA 算法作用）后，其结果或结果的一部分再与偏移量 411 进行运算（例如用 SHA 算法作用），最后取其输出作为算法 417 的输入密钥。这里叙述其步骤如下，

a）要生成口令时，动态口令生成器的微处理器执行以下步骤：

a1） 根据预先给定的长度和位置对动态变量进行分段，确定当前动态变量406的段始值407和偏移量411；

a2） 在步骤801对秘密密钥405、段始值407、偏移量411进行加密处理-1，得出第一动态密码419；在步骤802对秘密密钥405、动态变量406进行加密处理-2，得出第二动态密码420；

a3） 将动态密码419和动态密码420结合，构成动态口令421；

b） 将动态口令421传送至验证器。

c） 要验证口令时，验证器的微处理器执行以下步骤：

c1） 将接收到的动态口令421a分离成动态密码419a和动态密码420a；根据验证方动态变量在502估计段始值和偏移量范围；

c2） 在801a步骤对收到的动态密码419a、秘密密钥405a和在407a取得的估计段始值进行加密处理-1a，得到一个偏移量411a；

c3） 在503判断还原的偏移量411a是否在估计的偏移量范围内，若在允许的估计偏移量范围内，则执行406a步骤，由偏移量411a与在407a取得的估计段始值一起还原出一个动态变量，在802a步骤对秘密密钥405a和在406a还原的动态变量进行加密处理-2a，得到验证码420b，将验证码420b与所收到的动态密码420a 在511比较，若匹配则用户合法，在509允许用户访问，验证过程结束；若不匹配或该值所确定的偏移量不在所估计的偏移量范围内，则在504判断是否还有另外的估计段始值，若无则用户为非法，在505拒绝用户访问，验证过程结束；若有则取下一个估计段始值，转步骤c2）。

在步骤a2）中，还可对秘密密钥405、动态变量406和段始值407进行加密处理-2，得

出动态密码420；或对秘密密钥405、动态变量406、段始值407和偏移量411进行加密处理-2，得出动态密码420。

相应地，在步骤c3）中，还可对秘密密钥405a、在406a还原的动态变量和在407a取得的估计段始值进行加密处理-2a，得到验证码420b；或对秘密密钥405a、在406a还原的动态变量、在407a取得的估计段始值和偏移量411a进行加密处理-2a，得到验证码420b。

图 6 是验证器方在接收到用户的口令后，依据自己的时钟和信息库中有关信息，估计口令生成器方生成口令时动态变量时间的段始值和相应偏移量的范围，即就是对 502 过程的详细说明。在这里，应事先说明的是，验证器方所使用的基本时间单位、分段以及位置的确定等要求都应当与口令生成器方一致，前面已对它们作了说明，不再赘述。 验证器接收到用户的 ID 和口令后，先在 601 中记录此时的时间，并根据该时间确定动态变量 T。501 信息库中的 t 是该用户上一次，也就是最近一次口令生成器生成并已成功登录的动态口令所用的时间动态变量。t0 是该用户口令生成器初次生成并已成功登录的动态口令所用的时间动态变量。偏差 diff 就是最近一次口令生成器生成并已成功登录的动态口令所用的动态变量与当时在 601 中获得的时间确定动态变量 T 的差值(不妨设定为上次的 t 减去上次的 T，当然颠倒过来也可以，但意义相反)，它反映了该口令生成器时钟与验证器时钟的偏移程度，当 diff<0，表示验证器的时钟比该口令生成器的时钟相对地快 diff 个时间单位，反之则是慢 diff 个时间单位。为便于计算，这里的动态变量 T、t 和 t0 等可以相对于某一起始时间至该时的时间单位的个数来确定，例如假定以 2000 年 1 月 1 日 0 点整为起始参照时间，t0 由 2000 年 1 月 1 日 8 点整确定，t 由 2000 年 1 月 1 日 10 点整确定，T 由 2000 年 1 月 1 日 13 点整确定，则它们可以分别表示为 t0=480，t=600 以及 T=780。图 6 中，在 605 计算 t0 至 t 有多少个事先确定的时间周期长度(例如有 d1 个月，下面以月为周期长度说明)，对计算月的数量取整即可，当不足一个月时，取 0，不足两个月时，取 1，等等；在 604 计算 t 至 T 有多少个月(如 d2 个月)，在 606 利用已知的偏差 diff 估计在 d2 个月里会产生的偏差σ，当 d1 或者 d2 等于零时，设定σ等于 0，即无需考虑此偏差，否则计算σ =(diff/d1)×d2。在 607 根据 d2 的大小确定系统允许估计值误差的范围[c1，c2]，因为 d2 越大，影响时钟同步的不可预知的因素就会越多，各种估计值(如σ)的误差也会加大；可以根据实际需要和具体情况确定范围[c1，c2]，例如可如下设定其取值：

当 d2 = 0， 取 c1 = -2， c2 = +1；
当 d2 = 1， 取 c1 = -3， c2 = +2；
当 d2 = 2， 取 c1 = -3， c2 = +3；
.....

不难看出，范围[c1，c2]就决定了验证器方估计偏移量范围内的偏移量个数。另一种办法是，为了简化计算，可以省去σ的计算(即设定σ = 0)，并适当地将如上确定的[c1，c2]加以扩大即可，此时，就可以省去信息库中参数 t0。例如：

当 d2 = 0， 取 c1 = -2， c2 = +1；
当 d2 = 1， 取 c1 = -3， c2 = +3；
当 d2 = 2， 取 c1 = -4， c2 = +4；
.....

按口令生成器同样的分段标准，根据在 601 确定的动态变量 T，获得其偏移量 r 和段

始值 R，然后在 608 根据 606、607 和 603 步骤的结果计算出对偏移量的估计值，小的值 b1 = r + diff + σ + c1，大的值 b2 = r + diff + σ + c2。在 609，如果 b2<0，则在 610 取紧邻 R 之前的一个段始值 R1，偏移量范围取[b1+max，b2+max]，这里 max 表示最大偏移量值；否则在 611 如果 b1<0，则在 612 取段始值 R1，偏移量范围[b1+max，max]，和段始值 R，偏移量范围[0，b2]；否则在 613，如果 b1>max，则在 614 取紧邻 R 之后的一个段始值 R2，偏移量范围[b1-max，b2-max]；否则在 615，如果 b2>max，则在 616 取段始值 R2，偏移量范围[0，b2-max]，和段始值 R，偏移量范围[b1，max]；否则在 617 取段始值 R，偏移量范围[b1，b2]。以上判断顺序并不是唯一的，例如可先判定 b1 是否大于 max 等等，另外，也可以先以 diff 是否大于零为序进行判断。因此，这里判断的顺序和方式是次要的，主要的是这里总共只会出现 5 种可能发生的对段始值和偏移量的估计情况，并且只有两种情况下才会出现在 612 和在 616 中需估计两个段始值。

图 7 是验证器方在接收到用户的口令后，依据信息库中的信息，估计口令生成器方生成口令时，以口令生成次数为动态变量的段始值和相应偏移量的范围，即也是对 502 过程的详细说明。501 信息库中的 c 是该用户上一次，也就是最近一次口令生成器生成的已成功登录的口令所用的动态变量(即所用的生成口令的次数)。验证器 506 接收到用户的 ID 和口令后，在 701 从库中取出 c 值并将 c 值增一，按口令生成器同样的分段标准，取动态变量 c+1 的偏移量 r 和段始值 R，在 704 计算对偏移量的估计值，小的值 b1 = r，大的值 b2 = r + d，这里 d 值是事先确定的允许口令生成器连续生成的口令，而这些口令又没有在验证器方成功使用的次数，d 值可以是由系统统一确定，也可以是因不同的用户而具体确定，并且跟踪每个用户使用的情况来调整，其作用相当于基于时间动态变量中允许误差范围[c1，c2]，但是所确定的 d 值必须足小于已设定的段长度 L。在 707，如果 b2 大于 max，则在 708 取段始值 R，偏移量范围[b1，max]，和取紧邻 R 之后的一个段始值 R2，偏移量范围[0，b2-max]；否则在 709 取段始值 R，偏移量范围[b1，b2]。同上一样，这里判断的顺序和方式是次要的，主要的是这里共只会出现 2 种可能发生的对段始值和偏移量的估计情况，并且只有一种情况下才会出现在 708 中需估计两个段始值。

为了便于描述，在权利要求中使用了一些新的术语，这里将新术语与原有术语之间的对应关系说明如下：

新术语	原有术语
第一秘密密钥	秘密密钥 405
第二秘密密钥	秘密密钥 405a
第一动态变量	动态变量 406
第二动态变量	在 601 确定的动态变量 T，701 确定的动态变量
第三动态变量	在 406a 还原的动态变量
第一段始值	段始值 407
第二段始值	在 602 确定的段始值 R，703 确定的段始值 R
第一偏移量	偏移量 411
第二偏移量	在 603 确定的偏移量 r，702 确定的偏移量 r
第三偏移量	偏移量 411a
第一加密处理	在 801 实现的加密处理-1

第二加密处理	在 802 实现的加密处理-2
第三加密处理	在 801a 实现的加密处理-1a
第四加密处理	在 802a 实现的加密处理-2a
第一动态密码	动态密码 419
第二动态密码	动态密码 420
第三动态密码	动态密码 419a
第四动态密码	动态密码 420a
第一加密算法	算法 410
第二加密算法	算法 417
第三加密算法	算法 410a
第四加密算法	算法 417a
第一动态密钥	动态密钥 413
第二动态密钥	动态密钥 414
第三动态密钥	动态密钥 413a
第四动态密钥	动态密钥 414a
第五动态密钥	动态密钥 416
第六动态密钥	动态密钥 416a
第一动态变换表	动态变换表 418
第二动态变换表	动态变换表 418a
第一编码	编码 408
第二编码	编码 412
第三编码	编码 408a
第四编码	编码 412a

上面已结合各种特定实施例描述了本发明，熟悉本领域的技术人员将理解可在不脱离权利要求书中所陈述的发明精神与范围之下对其作出无数种变化，例如，动态口令的变化可以不止单一地由时间决定，或单一地由生成口令的次数决定，而是可以由时间和生成口令的次数这两个变化因素共同来决定动态口令的变化等。

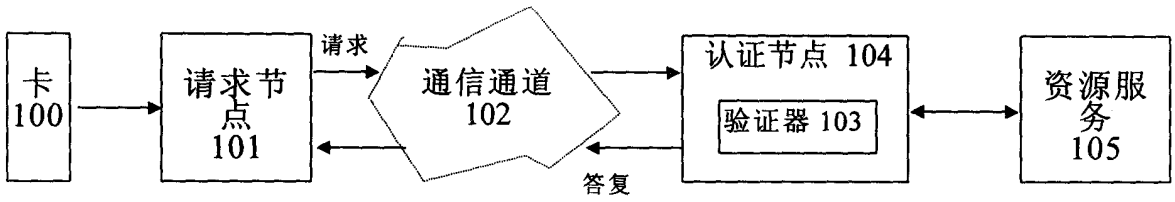

卡
100
请求节点
101
请求
通信通道
102
答复
认证节点 104
验证器 103
资源服务
105

图 1

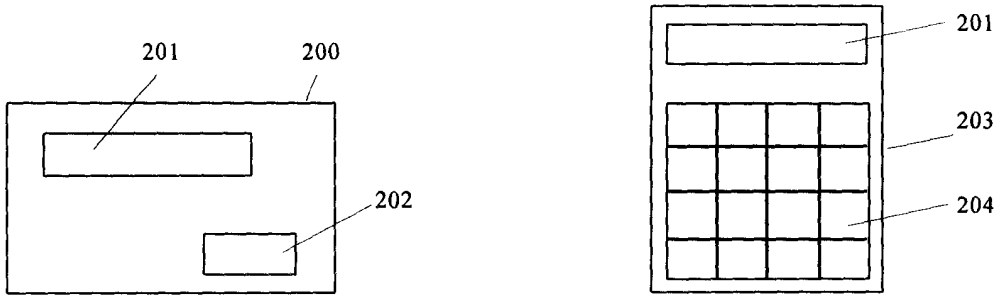

201
200
202
201
203
204

图 2

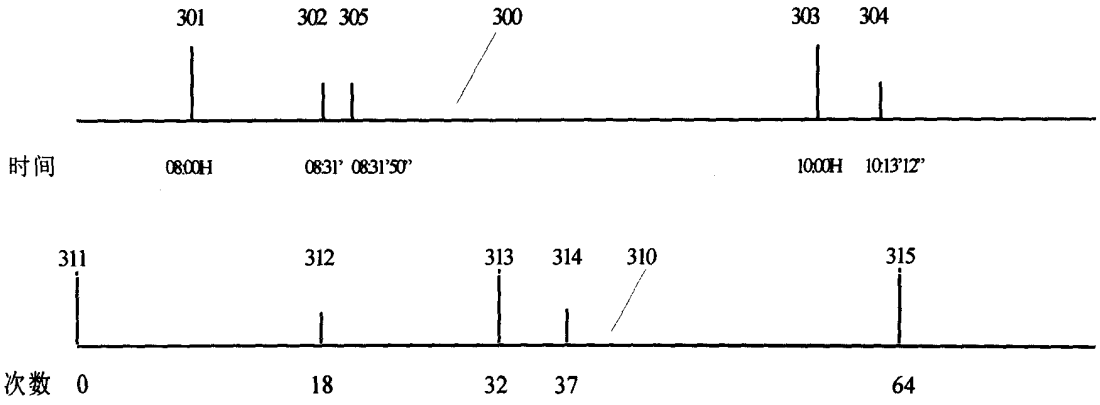

301
302 305
300
303
304
时间
08:00H
08:31' 08:31'50"
10:00H
10:13'12"
311
312
313
314
310
315
次数
0
18
32
37
64

图 3

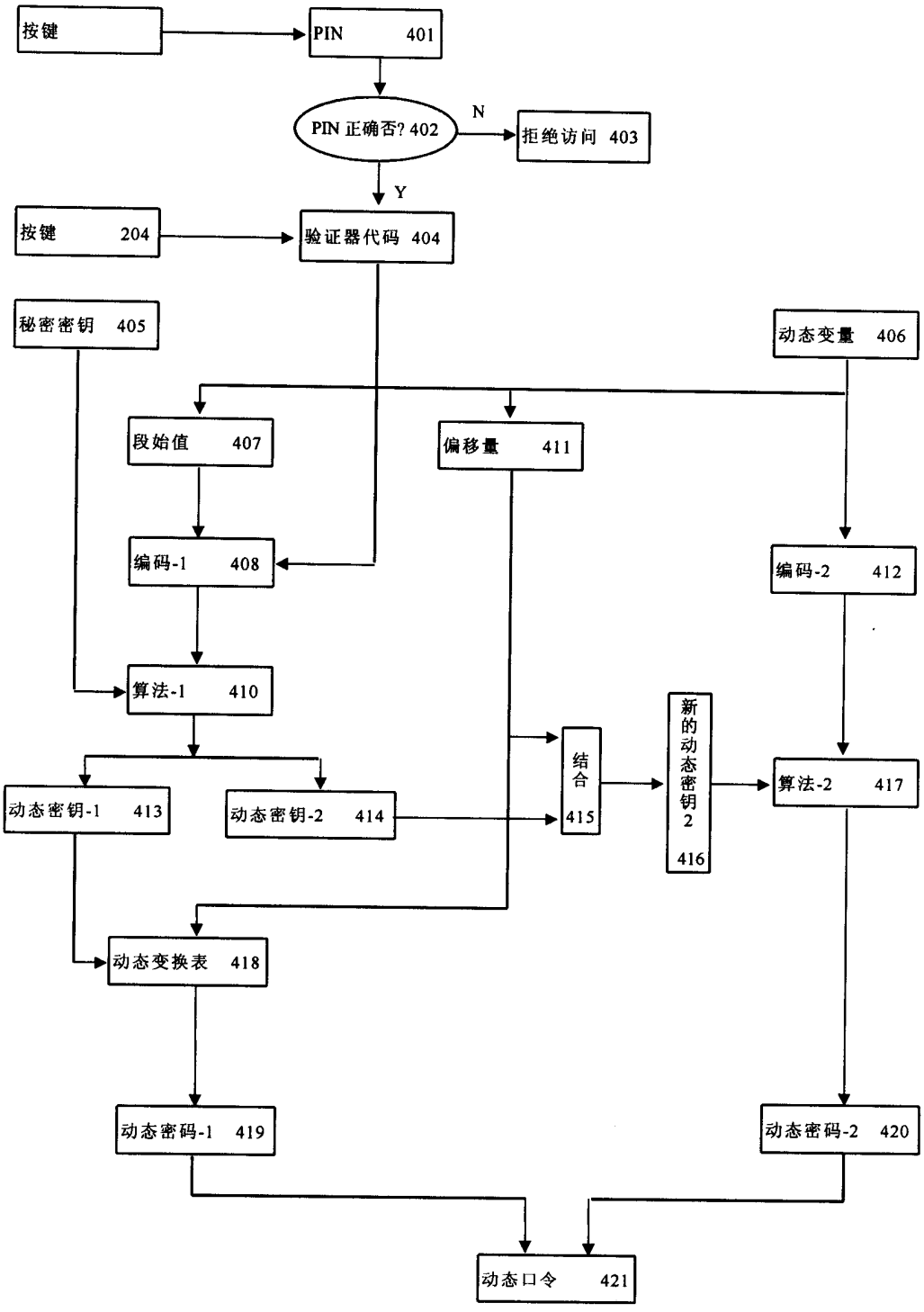

按键
PIN 401
PIN 正确否? 402
N
拒绝访问 403
Y
按键 204
验证器代码 404
秘密密钥 405
动态变量 406
段始值 407
偏移量 411
编码-1 408
编码-2 412
算法-1 410
结合 415
新的动态密钥2 416
算法-2 417
动态密钥-1 413
动态密钥-2 414
动态变换表 418
动态密码-1 419
动态密码-2 420
动态口令 421

图 4

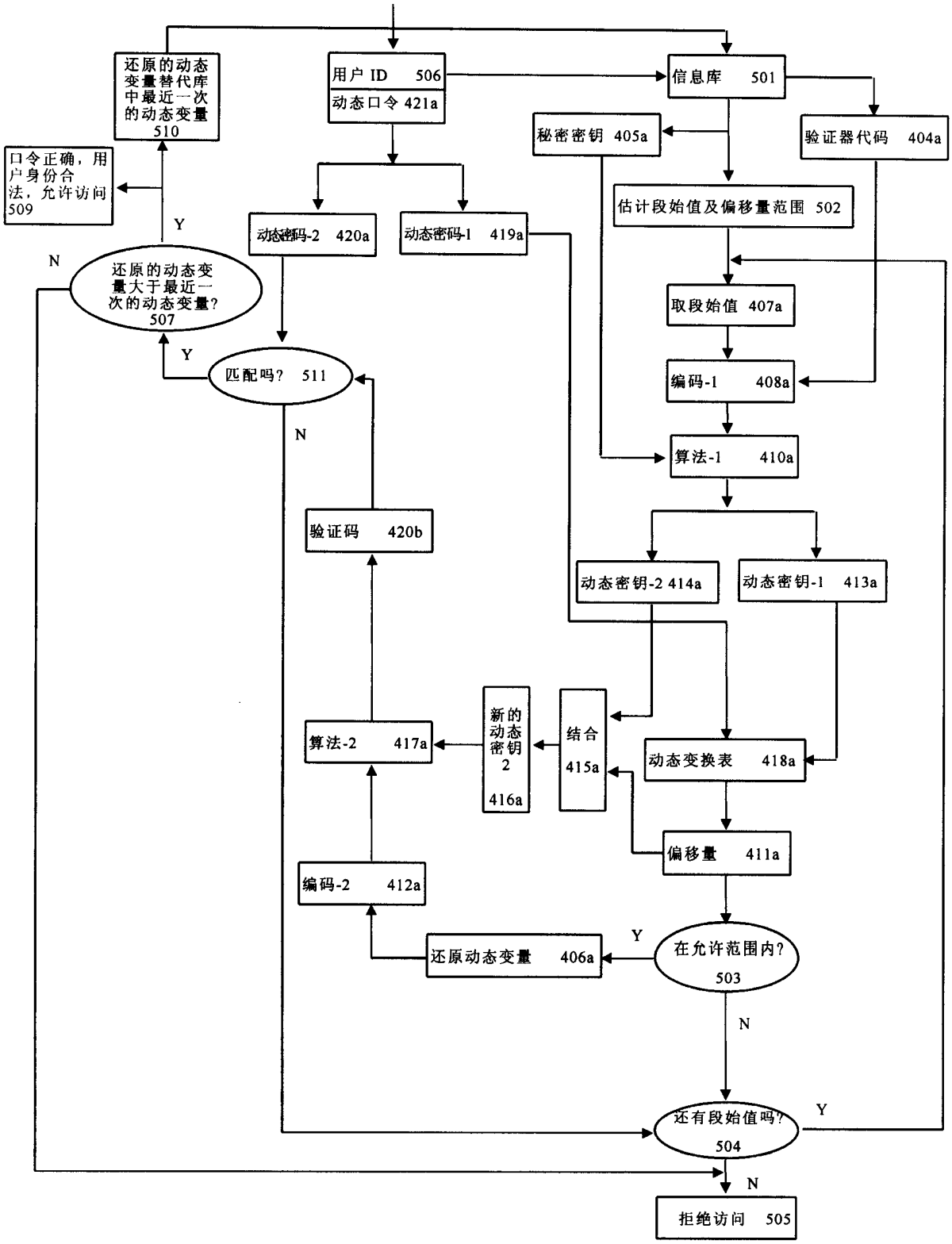

还原的动态变量替代库中最近一次的动态变量 510
用户 ID 506
动态口令 421a
信息库 501
秘密密钥 405a
验证器代码 404a
口令正确，用户身份合法，允许访问 509
Y
动态密码-2 420a
动态密码-1 419a
估计段始值及偏移量范围 502
N
还原的动态变量大于最近一次的动态变量? 507
取段始值 407a
Y
匹配吗? 511
编码-1 408a
N
算法-1 410a
验证码 420b
动态密钥-2 414a
动态密钥-1 413a
新的动态密钥 2 416a
结合 415a
算法-2 417a
动态变换表 418a
偏移量 411a
编码-2 412a
Y
还原动态变量 406a
在允许范围内? 503
N
Y
还有段始值吗? 504
N
拒绝访问 505

图 5

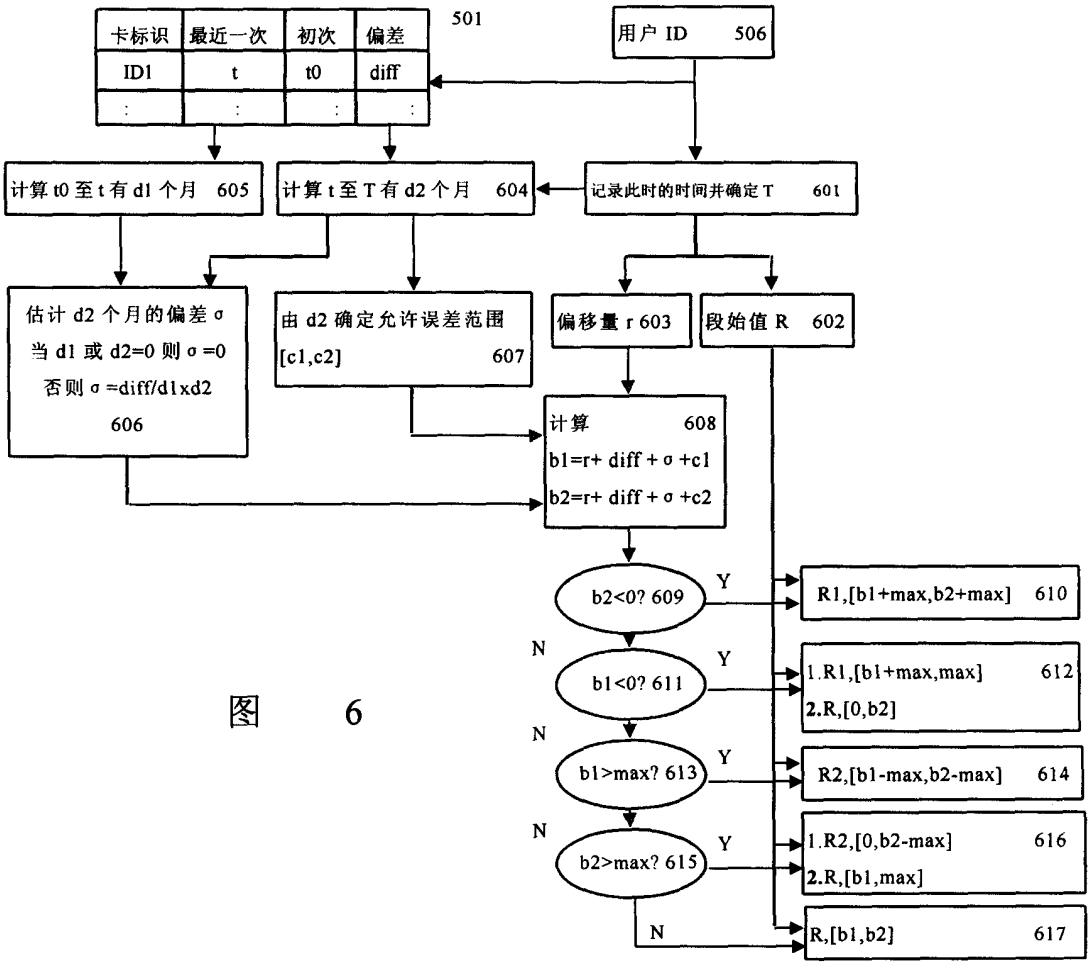

卡标识 最近一次 初次 偏差
ID1 t t0 diff
501
用户 ID 506
记录此时的时间并确定 T 601
计算 t0 至 t 有 d1 个月 605
计算 t 至 T 有 d2 个月 604
估计 d2 个月的偏差 σ
当 d1 或 d2=0 则 σ =0
否则 σ =diff/d1xd2
606
由 d2 确定允许误差范围
[c1,c2] 607
偏移量 r 603
段始值 R 602
计算 608
b1=r+ diff + σ +c1
b2=r+ diff + σ +c2
b2<0? 609
R1,[b1+max,b2+max] 610
b1<0? 611
1.R1,[b1+max,max] 612
2.R,[0,b2]
b1>max? 613
R2,[b1-max,b2-max] 614
b2>max? 615
1.R2,[0,b2-max] 616
2.R,[b1,max]
R,[b1,b2] 617
Y
N

图 6

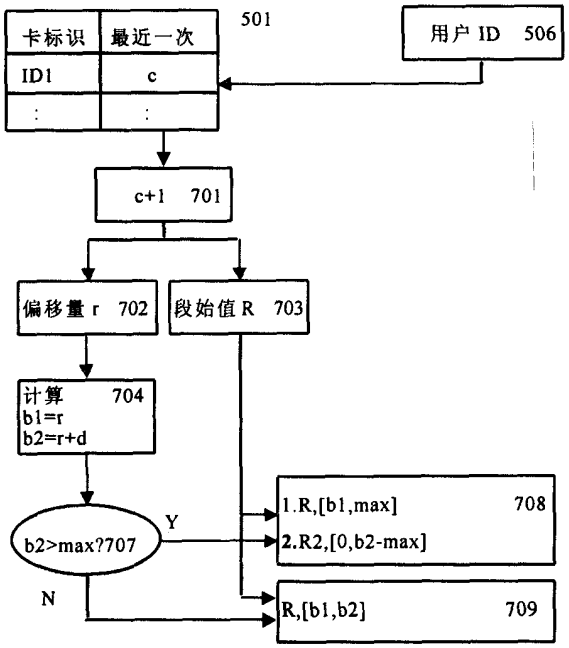
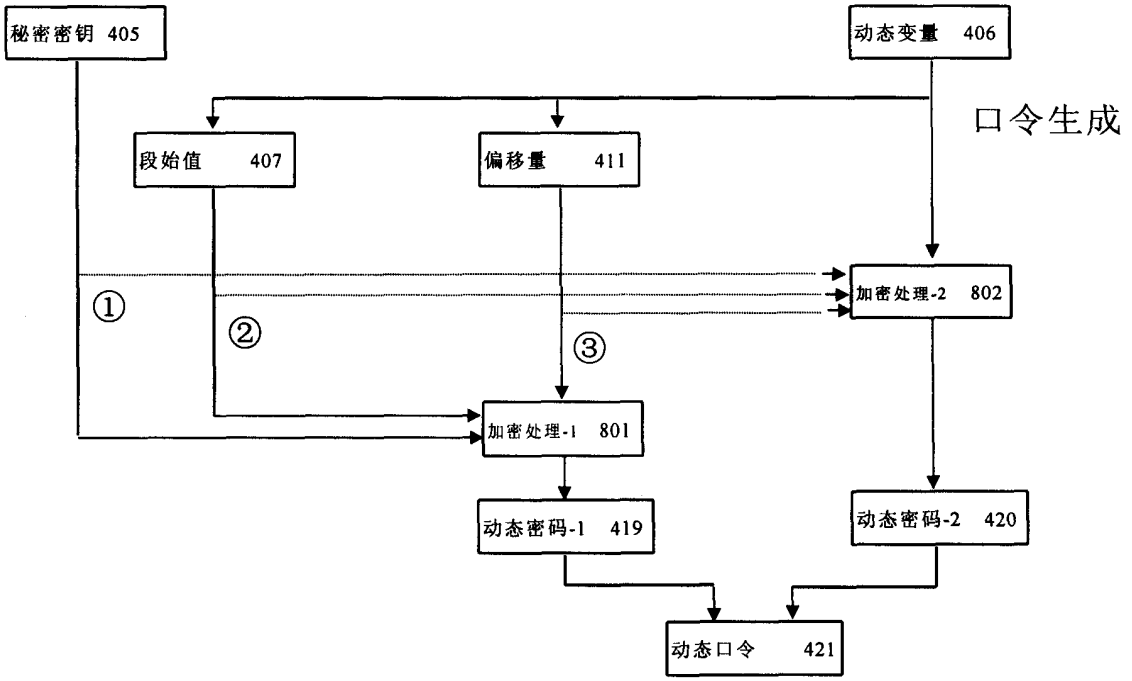

卡标识 最近一次
ID1 c
501
用户 ID 506
c+1 701
偏移量 r 702
段始值 R 703
计算 704
b1=r
b2=r+d
b2>max?707
1.R,[b1,max] 708
2.R2,[0,b2-max]
R,[b1,b2] 709
Y
N

图 7


秘密密钥 405
动态变量 406
口令生成
段始值 407
偏移量 411
①
②
③
加密处理-2 802
加密处理-1 801
动态密码-1 419
动态密码-2 420
动态口令 421

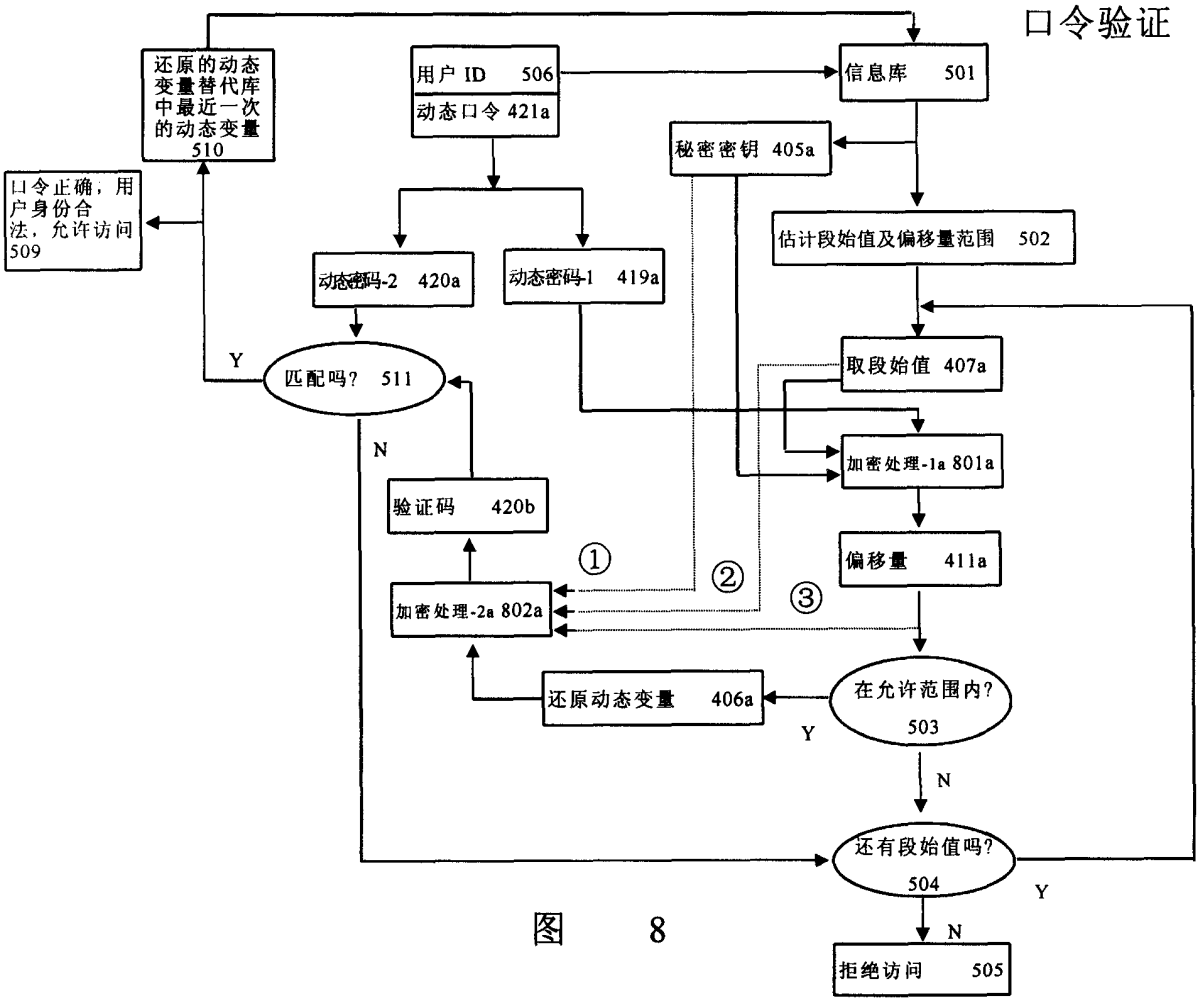

口令验证
还原的动态变量替代库中最近一次的动态变量 510
用户 ID 506
动态口令 421a
信息库 501
秘密密钥 405a
口令正确，用户身份合法，允许访问 509
估计段始值及偏移量范围 502
动态密码-2 420a
动态密码-1 419a
取段始值 407a
Y
匹配吗？ 511
N
加密处理-1a 801a
验证码 420b
偏移量 411a
①
②
③
加密处理-2a 802a
还原动态变量 406a
在允许范围内？ 503
Y
N
还有段始值吗？ 504
Y
N
拒绝访问 505

图 8