

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.  
H04L 9/08 (2006.01)



# [12] 发明专利申请公布说明书

[21] 申请号 200880010601.3

[43] 公开日 2010年2月10日

[11] 公开号 CN 101647228A

[22] 申请日 2008.4.1

[21] 申请号 200880010601.3

[30] 优先权

[32] 2007.4.5 [33] EP [31] 07105710.3

[86] 国际申请 PCT/IB2008/051216 2008.4.1

[87] 国际公布 WO2008/122923 英 2008.10.16

[85] 进入国家阶段日期 2009.9.29

[71] 申请人 国际商业机器公司

地址 美国纽约

[72] 发明人 M·本特施 P·布勒 T·艾里希  
T·克兰普 T·D·威戈尔德

[74] 专利代理机构 北京市金杜律师事务所  
代理人 吴立明

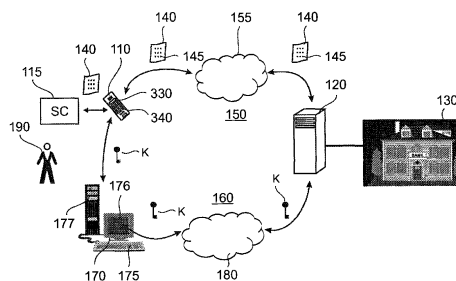
权利要求书6页 说明书30页 附图11页

## [54] 发明名称

用于证书分发的系统和方法

## [57] 摘要

本发明涉及一种用于将证书集合从证书签发方分发给证书用户的方法，其中证书用户具有用户设备，其中，提供第一信道和第二信道用于用户设备与证书签发方之间的通信，该方法包括步骤：借助第二信道在用户设备与证书签发方之间分发共享密钥，生成相对于均匀分布具有预定义最大偏差水平的、证书集合的二进制表示，借助共享密钥来加密对证书集合的二进制表示，经由第一信道将加密的证书集合从证书签发方分发给用户设备，用户设备借助共享密钥对加密的证书集合进行解密。



1. 一种用于将证书(145)集合(140)从证书签发方(130)分发给证书用户(190)的方法,其中所述证书用户(190)具有用户设备(110),其中,提供第一信道(150)和第二信道(160)用于所述用户设备(110)与所述证书签发方(130)之间的通信,所述方法包括步骤:

- 借助所述第二信道(160)在所述用户设备(110)与所述证书签发方(130)之间分发共享密钥(K),

- 生成相对于均匀分布具有预定义最大偏差水平的、所述证书(145)集合(140)的二进制表示,

- 借助所述共享密钥(K)来加密所述证书(145)集合(140)的所述二进制表示,

- 经由所述第一信道(150)将所述加密的证书(145)集合(140)从所述证书签发方(130)分发给所述用户设备(110),

- 所述用户设备(110)借助所述共享密钥(K)来解密所述加密的证书(145)集合(140)。

2. 根据权利要求1所述的方法,还包括步骤:将经解密的证书(145)从所述证书用户(190)提供给所述证书签发方(130)以进行验证,其中提供所述签证签发方(130)以用于仅允许预定义次数的验证试探。

3. 根据权利要求1或者2所述的方法,其中对所述证书(145)集合(140)的所述二进制表示相对于均匀分布的所述预定义最大偏差水平取决于:预定义安全水平、所述共享密钥(K)的密钥长度以及预定义的验证试探次数。

4. 根据任一前述权利要求所述的方法,其中所述共享密钥(K)是弱密钥。

5. 根据任一前述权利要求所述的方法,其中所述第二信道(160)包括人工用户接口(340, 175)。

6. 根据任一前述权利要求所述的方法，还包括步骤：

- 所述用户设备（110）生成和显示所述共享密钥（K），
- 所述认证用户（190）在又一设备（170）上人工录入所述共享密钥（K），
- 将所述共享密钥（K）从所述又一设备（170）传送到所述证书签发方（130）。

7. 根据任一前述权利要求所述的方法，还包括步骤：

- 所述证书签发方（130）生成所述共享密钥（K），
- 将所述共享密钥（K）从所述证书签发方（130）传送到所述又一设备（170），
- 所述又一设备（170）显示所述共享密钥（K），
- 所述证书用户（190）在所述用户设备（110）上人工录入所述共享密钥（K）。

8. 根据任一前述权利要求所述的方法，其中所述证书（145）包括预定义数目的证书符号，并且所述证书符号是证书字符表的元素。

9. 根据权利要求8所述的方法，其中所述证书字符表的规模选择为2的幂。

10. 根据任一前述权利要求所述的方法，还包括步骤：将噪声符号添加到所述证书（145）集合（140）。

11. 根据权利要求10所述的方法，其中所述噪声符号取自于包含证书符号以及一个或者多个噪声符号的噪声字符表，其中所述噪声字符表的规模选择为2的幂。

12. 根据权利要求11所述的方法，还包括步骤：

- 生成包括预定义数目的证书符号的证书（145）集合（140），
- 生成随机消息，其包含取自于所述噪声字符表的伪证书符号和噪声符号，其中所述伪证书符号的数目大于或者等于所述证书（145）集合（140）的证书符号的所述预定义数目，
- 在所述随机消息中，将所述伪证书符号的预定义集合替换为所

述证书（145）集合（140）的所述证书符号，

- 生成所述随机消息的二进制表示，由此建立相对于均匀分布具有所述预定义最大偏差水平的、所述证书（145）集合（140）的二进制表示。

13. 根据任一前述权利要求所述的方法，其中生成相对于均匀分布具有所述预定义最大偏差水平的、所述证书（145）集合（140）的所述二进制表示包括子步骤：

- 生成具有第一随机水平的、所述证书（145）集合（140）的第一表示，

- 将所述第一表示变换成具有第二随机水平的、所述证书（145）集合（140）的第二表示，其中所述第二随机水平高于所述第一随机水平，

- 将所述证书（145）集合（140）的所述第二表示变换成相对于平均分布具有所述预定义最大偏差水平的所述二进制表示。

14. 根据任一前述权利要求所述的方法，其中所述证书（145）集合（140）被划分成用于二进制转换的单位，其中以如下方式来选择所述用于二进制转换的单位，即，不代表证书符号的二进制表示的比例小于预定义比例。

15. 根据任一前述权利要求所述的方法，其中所述证书（145）集合（140）被划分成用于二进制转换的单位，每个单位包括两个或者更多证书符号。

16. 根据任一前述权利要求所述的方法，其中所述第一信道（150）是非信任信道，而所述第二信道（160）是受信任信道。

17. 根据任一前述权利要求所述的方法，其中所述证书（145）是一次性认证码。

18. 根据任一前述权利要求所述的方法，其中所述第一信道（150）是无线通信信道，而所述第二信道（160）包括安全因特网连接、电话线和邮件服务之一。

19. 根据任一前述权利要求所述的方法，其中所述用户设备

(110) 包括移动电话和个人数字助理之一。

20. 一种用于将证书(145)集合(140)从证书签发方(130)分发给证书用户(160)的方法,其中所述证书用户(190)具有用户设备(110),其中,提供第一信道(150)和第二信道(160)用于所述用户设备(110)与所述证书签发方(130)之间的通信,其中所述方法在证书服务器(120)中包括步骤:

- 生成共享密钥(K)并且将所述共享密钥(K)分发给所述用户设备(110),或者经由所述第二信道(160)从所述用户设备(110)接收共享密钥,

- 生成相对于均匀分布具有预定义最大偏差水平的、所述证书(145)集合(140)的二进制表示,

- 借助所述共享密钥(K)来加密所述证书(145)集合(140)的所述二进制表示,

- 经由所述第一信道(150)将所述加密的证书(145)集合(140)分发给所述用户设备(110)。

21. 一种包括指令的计算程序,所述指令用于在所述计算机程序在计算机系统上执行时实现根据权利要求20所述的方法的步骤。

22. 一种用于用户设备(110)从证书服务器(120)接收证书(145)集合(140)的方法,其中,提供第一信道(150)和第二信道(160)用于所述用户设备(110)与所述证书服务器(120)之间的通信,其中所述方法在所述用户设备(110)中包括步骤:

- 生成共享密钥(K)并且将所述共享密钥(K)分发给所述证书服务器(120),或者经由所述第二信道(160)从所述证书服务器(120)接收共享密钥(K),

- 接收相对于均匀分布具有预定义最大偏差水平的、所述证书(145)集合(140)的二进制表示,其中所述证书(145)集合(140)的所述二进制表示是借助所述共享密钥(K)而加密的,

- 借助所述共享密钥(K)来解密所述加密的证书(145)集合(140),

- 存储所述解密的证书 (145) 集合 (140)。

23. 一种包括指令的计算程序, 所述指令用于在所述计算机程序在计算机系统中执行时实现根据权利要求 22 所述的方法的步骤。

24. 一种用于经由非信任信道 (150) 将证书 (145) 集合 (140) 从证书签发方 (130) 安全地发送到证书用户 (190) 的方法, 所述方法包括步骤:

- 生成相对于均匀分布具有预定义最大偏差水平的、所述证书 (145) 集合 (140) 的二进制表示,

- 借助共享密钥 (K) 来加密所述证书 (145) 集合 (140) 的所述二进制表示,

- 经由所述非信任信道 (150) 将所述加密的证书 (145) 集合 (140) 从所述证书签发方 (130) 发送到所述证书用户 (190)。

25. 一种包括指令的计算程序, 所述指令用于在所述计算机程序在计算机系统中执行时实现根据权利要求 24 所述的方法的步骤。

26. 一种用于将证书 (145) 集合 (140) 从证书签发方 (130) 分发给证书用户 (190) 的系统 (100), 其中所述证书用户 (190) 具有用户设备 (110), 其中, 提供第一信道 (150) 和第二信道 (160) 用于所述用户设备 (110) 与所述证书签发方 (130) 之间的通信, 提供所述系统 (100) 以用于:

- 借助所述第二信道 (160) 在所述用户设备 (110) 与所述证书签发方 (130) 之间分发共享密钥 (K),

- 生成相对于均匀分布具有预定义最大偏差水平的、所述证书 (145) 集合 (140) 的二进制表示,

- 借助所述共享密钥 (K) 来加密对所述证书 (145) 集合 (140) 的所述二进制表示,

- 经由所述第一信道 (150) 将所述加密的证书 (145) 集合 (140) 从所述证书签发方 (130) 分发给所述用户设备 (110),

- 所述用户设备 (110) 借助所述共享密钥 (K) 来解密所述加密的证书 (145) 集合 (140)。

27. 一种用于将证书(145)集合(140)分发给证书用户(190)的证书服务器(120),其中所述证书用户(190)具有用户设备(110),其中,提供第一信道(150)和第二信道(160)用于所述用户设备(110)与所述证书服务器(120)之间的通信,提供所述证书服务器(120)以用于:

- 生成共享密钥(K)并且将所述共享密钥(K)分发给所述用户设备(110),或者经由所述第二信道(160)从所述用户设备(110)接收共享密钥(K),

- 生成相对于均匀分布具有预定义最大偏差水平的、所述证书(145)集合(140)的二进制表示,

- 借助所述共享密钥(K)来加密所述证书(145)集合(140)的所述二进制表示,

- 经由所述第一信道(160)将所述加密的证书(145)集合(140)从所述证书签发方(130)分发给所述用户设备(110)。

28. 一种被提供用于从证书服务器(120)接收证书(145)集合(140)的用户设备(110),其中,提供第一信道(150)和第二信道(160)用于所述用户设备(110)与所述证书服务器(120)之间的通信,提供所述用户设备(110)以用于:

- 生成共享密钥(K)并且将所述共享密钥(K)分发给所述证书服务器(120),或者经由所述第二信道(160)从所述证书服务器(120)接收共享密钥(K),

- 接收相对于均匀分布具有预定义最大偏差水平的、所述证书(145)集合(140)的二进制表示,其中所述证书(145)集合(140)的所述二进制表示是借助所述共享密钥(K)而加密的,

- 借助所述共享密钥(K)来解密所述加密的证书(145)集合(140),

- 存储所述解密的证书(145)集合(140)。

## 用于证书分发的系统和方法

### 技术领域

本发明涉及用于将一个或者多个证书从证书签发方分发给证书用户的方法。本发明还涉及相应系统、相应服务器、相应用户设备和相应计算机程序。

### 背景技术

证书可以例如是一次性认证码(OTAC)，例如交易号(TAN)。另外，证书可以例如是个人标识号(PIN)、口令、激活码或者强密钥材料。

在在线交易领域中流行一次性认证码，这些认证码具有事务认证号的基于纸介的刮擦(scratch)列表。基于纸介的刮擦列表既不很安全又不便于获取。通常，刮擦列表经由普通邮件从服务提供方如银行发送到客户。邮寄的刮擦列表可能在途中被截获并且被复制。此外，不能指望许多客户将刮擦列表存放于安全位置，例如保险箱中。在频繁使用刮擦列表的情况下尤其如此。频繁使用的刮擦列表可能因被遗忘而公开，例如遗忘在桌上。这给他人提供了获取刮擦列表之机。如果刮擦列表由客户携带，则其可能遗失或者被盗。通常，刮擦列表上的OTAC没有进行加密。客户账号通常与OTAC相结合来实现交易，客户账号被广泛认为是公开的。对于许多客户而言，人工跟踪已经使用哪些OTAC是不方便的。当从一个刮擦列表移动到另一刮擦列表时，客户需要暂时存放或者携带两个刮擦列表。这使安全风险提高。另外，签发服务提供方以及时的方式打印和邮寄基于纸介的刮擦列表颇为复杂。

WO98/37524描述一种使用移动设备的交易方法。这一方法运用国际借记用户标识(IDUI)号来标识个体账户。IDUI类似于客户



银行账号。具体而言，将 IDUI 预加载到借记/信用卡上。在操作中，销售点（POS）终端从借记卡/信用卡读取 IDUI，并且显示将从所标识账户扣除的数额。客户通过按动 POS 终端的确认按钮来完成交易。POS 终端将交易收据发送到负责账户的银行中的服务器。WO98/37524 提出将 IDUI 预存于例如在 GSM 移动电话网络中使用的用户标识模块（SIM）智能卡上，而不是磁条或者记忆卡上。终端继而以无接触方式从智能卡读取 IDUI。通过 SMS 消息将交易收据发送到服务器进行验证。这一方案仅讨论将 IDUI 用于经由无接触接口与 POS 终端的交易并且交换 SMS 消息进行交易验证。该方案并不适合于 OTAC 投递。这是因为 IDUI 对于各账户而言是固定的。然而，OTAC 并非如此。在 EP1 176 844、WO99/16029、WO00/495585、WO01/09851、WO02/21464 和 WO01/93528 中描述类似电子支付系统。

EP 1559256 B1 描述一种将一组访问码提供给用户设备的方法。根据这一方法，将强对称密钥如 16 字节的数据加密标准（DES）密钥用于对访问码的加密。

本发明的一个目的在于提供用于证书分发的其它解决方案。

本发明的又一目的在于提供用于从证书签发方到证书用户的证书初始分发的解决方案。

本发明的又一目的在于提供用于分发广泛适用的证书的解决方案。

本发明的又一目的在于提供用于证书分发的、广泛适用的解决方案。

## 发明内容

本发明涉及如在独立权利要求中限定的方法、系统、服务器、用户设备和计算机程序。

根据本发明的第一方面，提供一种用于将证书集合从证书签发方分发给证书用户的方法，其中证书用户具有用户设备，其中提供

第一信道和第二信道用于用户设备与证书签发方之间的通信，该方法包括步骤：

- 借助第二信道在用户设备与证书签发方之间分发共享密钥，
- 生成相对于均匀分布具有预定义最大偏差水平的证书集合的二进制表示，
- 借助共享密钥来加密证书集合的二进制表示，
- 经由第一信道将加密的证书集合从证书签发方分发给用户设备，
- 用户设备借助共享密钥对加密的证书集合进行解密。

借助相对于均匀分布的预定义最大偏差水平，可以限定证书集合的二进制表示可包括多少冗余。换言之，借助相对于均匀分布的预定义最大偏差水平，可以限定集合证书的二进制表示可包括多少结构。另外，借助相对于均匀分布的预定义最大偏差水平，可以限定或者指定证书集合的二进制表示具有 0 和 1 的分布，其与相应应用或者系统的安全性需求的均匀性充分接近。在证书集合的二进制表示中设置相对于均匀分布的预定义最大偏差水平，这增强了证书集合的分发安全性。证书集合的二进制表示可以具有相对于平均分布的最大偏差水平，但是也可以具有相对均匀分布的较低偏差水平。相对于均匀分布的最大偏差水平越低，证书集合的二进制表示与 0 和 1 的均匀分布越接近，证书集合所包括的结构越少并且冗余越少，而且证书集合越不容易受强力密钥搜索攻击的影响。换言之，攻击方无法依赖于结构信息来自行确定证书集合是否已经由试探密钥正确地解密。

设置相对于均匀分布的预定义最大偏差水平，这限定在其他方式下未知或不可靠或未确定的与安全性相关的变量。这允许根据相对于均匀分布的这一预定义最大偏差水平来设置证书分发系统的与安全性相关的其它变量。这同样允许对证书分发系统的更灵活设计。优选地，证书签发方将根据各自的应用来设置、确定或者选择相对于均匀分布的预定义最大偏差水平。

特别地，为二进制表示设置相对于均匀分布的预定义最大偏差水平允许减小共享密钥的密钥长度。

根据本发明的一个实施例，相对于均匀分布的最大偏差水平为零或者接近零。换言之，证书集合的二进制表示均匀地分布或者接近均匀分布。

根据本发明的一个实施例，相对于均匀分布的预定义最大偏差水平可以由一组随机性测试来限定或者确定，这些测试包括其各自的配置，这些配置将生成的证书集合的二进制表示认可为充分地随机、即充分均匀地分布。

根据本发明的一个实施例，相对于均匀分布的预定义最大偏差水平相应地确定如下测试密钥的百分比或者由该百分比限定，这些测试密钥可能由于试探解密获得无效证书集合（即获得看起来不像有效证书集合的解密消息）这一事实而被强力攻击所排除。

根据本发明的一个实施例，以如下方式来设置相对于均匀分布的预定义最大偏差水平，即使证书集合的二进制表示的随机水平大于零。

根据本发明的一个实施例，将相对于均匀分布的预定义最大偏差水平限定为证书集合的二进制表示的预定义最小随机水平。

根据本发明第一方面的一个实施例，该方法还包括步骤：将解密的证书从证书用户提供给证书签发方进行验证，其中提供证书签发方是为了仅允许预定义次数的验证试探。

预定义的验证试探次数越少，攻击方可能在证书签发方停用相应账户之前发现共享密钥的可能性就越小。由于证书的二进制表示包括相对于均匀分布的预定义最大偏差水平，所以借助于利用试探共享密钥解密的样本的输出结构，攻击方无法排除共享密钥或者仅能排除数目很少的共享密钥。换言之，攻击方需要验证证书签发方的验证反馈来验证所选试探共享密钥是否匹配或者是否可以被排除。

根据本发明第一方面的一个实施例，证书集合的二进制表示相

对于均匀分布的预定义最大偏差水平取决于预定义安全水平、共享密钥的密钥长度以及预定义的验证试探次数。

根据本发明第一方面的这一实施例，根据三个不同参数来选择或者确定或者设置相对于均匀分布的预定义最大偏差水平。预定义安全水平适于作为第一参数。这一预定义安全水平可以由证书签发方设置或者选择，并且可以由强力密钥搜索攻击成功的概率来限定。优选地，证书签发方将根据应用和其客户的需求来设置或者确定预定义安全水平。

确定或者影响相对于均匀分布的预定义最大偏离水平的第二参数是共享密钥的密钥长度。共享密钥越长，密钥空间越大，并且进行强力密钥搜索攻击的攻击方需要从中进行选择的试探密钥越多。

确定或者影响相对于均匀分布的预定义最大偏离水平的第三参数是预定义的验证试探次数。预定义的验证试探次数越小，强力密钥搜索攻击成功的可能性越小。

所有这三个参数交互地影响或者确定相对于均匀分布的预定义最大偏差水平。

根据本发明第一方面的一个实施例，共享密钥是弱密钥。

将弱密钥理解为相对于强力密钥搜索攻击（即对密钥空间的强力搜索）弱加密密钥。这样的强力密钥搜索攻击可以基于证书集合的二进制表示，该二进制表示包括用以排除错误试探密钥的充分的冗余或者结构水平的对。这样的强力密钥搜索攻击可以由对包含证书集合的消息进行截获的中间攻击方来进行。攻击方可以尝试通过分析所得输出的结构来区分解密的样本。换言之，攻击方知道包含证书集合的纯文本消息具有某一结构或者字符分布。可以排除没有产生这一已知结构或者字符分布、而产生 0 和 1 的均匀或者接近均匀分布的对弱密钥的错误猜测。

就这样的强力密钥搜索攻击而言，依赖于所用密钥的长度，存在对抗攻击的防范连续性。换言之，根据本发明一个实施例的弱

密钥是具有小密钥尺寸或者短密钥长度的密钥。通常，如果强力攻击实现起来在计算上不可行，则将密钥视为弱密钥。

一般而言，随着计算能力的技术发展，被视为强加密密钥的密钥的密钥长度将变得越来越长，并且相应地，被视为弱密钥的密钥的密钥长度也将变得越来越长。

目前对于许多应用来说，将强加密密钥视为具有至少 112 位的密钥、例如 2 个密钥-三重 DES（数据加密标准）密钥。因而，将根据本发明一个实施例的弱密钥理解为具有少于 112 位的密钥。

高级加密标准（AES）目前使用最少 128 位的密钥规模。因而，将根据本发明另一实施例的弱密钥理解为具有少于 128 位的密钥。

美国政府将 192 或者 256 位的 AES 密钥用于绝密数据。因而，将根据本发明另一实施例的弱密钥理解为具有少于 192 或者 256 位的密钥。

将弱密钥用于对证书集合进行加密具有的优点在于，其促进了某些软件在用户设备上设置或者定制期间的用户输入。这对于小键盘或者显示器有限的用户设备（如移动电话）而言特别地有用。

根据本发明的一个实施例，共享密钥包括 10 位或者少于 10 位。根据本发明的另一实施例，共享密钥包括 50 位或者少于 50 位。根据本发明的另一实施例，共享密钥包括 100 位或者少于 100 位。可以根据证书集合的二进制表示相对于均匀分布的预定义最大偏差水平、预定义安全水平和预定义验证试探次数，来选择相应的密钥长度。通过为证书集合的二进制表示设置相对于均匀分布的预定义最大偏差水平，有助于使用这样的短共享密钥。

根据本发明第一方面的一个实施例，第二信道包括人工用户接口。可以在用户设备上提供人工用户接口。在第二信道中提供人工用户接口具有的优点在于该方法可广泛地适用，因为人工用户接口是多数电子设备的一部分。

根据本发明第一方面的一个实施例，该方法还包括步骤：

- 用户设备生成和显示共享密钥，

- 证书用户在又一设备上人工录入共享密钥，
- 将共享密钥从所述又一设备传送到证书签发方。

在这一实施例中，共享密钥由用户设备生成、然后分发给证书签发方。这给予了证书用户增强的灵活性，并且允许他自发地启动共享密钥分发。特别地，又一设备可以是计算机。

根据本发明第一方面的一个实施例，该方法还包括步骤：

- 证书签发方生成共享密钥，
- 将共享密钥从证书签发方传送到又一设备，
- 所述又一设备显示共享密钥，
- 用户在用户设备上人工录入共享密钥。

在这一实施例中，共享密钥由证书签发方生成、然后分发给证书用户的用户设备。这给予了证书用户增强的灵活性。特别地，又一设备可以是计算机。

根据本发明第一方面的一个实施例，证书包括预定义数目的证书符号，并且证书符号是证书字符表的元素。

作为示例，证书可以由例如 6 个十进制数构成的交易号 (TAN)。在本例中，十进制数 0-9 是建立证书字符表的证书符号。

根据本发明第一方面的一个实施例，证书字符表的规模选择为 2 的幂。

这样做的优点在于，可以在没有任何冗余或者结构的情况下实施证书符号的二进制表示。换言之，每个证书符号对应于具体的二进制表示。所选二进制编码方案并不包括不与有效证书对应的二进制表示。

作为示例，证书字符表可以由 16 个十六进制数 0-9 以及 A-F 建立。将这些十六进制数中的每个十六进制数转换成 4 位的二进制 (二元) 表示。这些 4 位有  $2^4 = 16$  个二进制组合，并且每个组合对应于一个十六进制数。

根据本发明第一方面的一个实施例，该方法还包括将噪声符号添加到证书集合的步骤。

噪声符号是没有代表有效证书的符号。添加噪声符号的优点在于，进行强力攻击的攻击方不能简单地排除未对应有效证书符号的二进制表示。

根据本发明第一方面的一个实施例，噪声符号取自于由证书符号以及一个或者多个噪声符号构成的噪声字符表，其中噪声字符表的规模选择为2的幂。

作为示例，证书符号可以由十六进制的十进制数数字0-9代表，而噪声符号由字符A-F代表。根据这一符号表示，包括证书符号0-9和噪声符号A-F的整个十六进制字符表建立噪声字符表。

使用规模为2的幂的噪声字符表具有的优点在于，可以在没有任何冗余或者结构的情况下实施噪声字符表的二进制表示。换言之，每个证书符号和每个噪声符号对应于具体的二进制表示，并且所选二进制编码方案并不包括不与噪声符号或者证书符号对应的二进制表示。

根据本发明第一方面的一个实施例，该方法还包括步骤：

- 生成包括预定义数目的证书符号的证书集合，
- 生成由取自于噪声字符表的伪(dummy)证书符号和噪声符号构成的随机消息，其中伪证书符号的数目大于或者等于证书集合的证书符号的预定义数目，
- 在随机消息中利用证书集合的证书符号替换伪证书符号的预定义集合，
- 生成随机消息的二进制表示，由此建立相对于均匀分布具有预定义最大偏差水平的证书集合的二进制表示。

本发明的这一实施例具有的优点在于，可以独立于二进制表示的生成来执行证书集合的生成。这允许由与执行二进制表示生成的单元或者实体分离的单元或者实体来生成证书集合。这允许在安全和封闭环境中生成证书集合，并且对执行证书集合生成的算法加以保密。

作为示例，第一处理单元可以执行证书集合的生成。该第一处

理单元可以布置于证书签发方的高安全区中。第一处理单元将该证书集合发送或者转发到第二处理单元，提供该第二处理单元是为了生成相对于均匀分布具有预定义最大偏差水平的证书集合的二进制表示。

根据本发明第一方面的一个实施例，生成相对于均匀分布具有预定义最大偏差水平的证书集合的二进制，表示包括子步骤：

- 生成具有第一随机水平的证书集合的第一表示，
- 将第一表示变换成具有第二随机水平的证书集合的第二表示，其中第二随机水平高于第一随机水平，
- 将证书集合的第二表示变换成相对于平均分布具有预定义最大偏差水平的二进制表示。

根据本发明的这一实施例，通过三个步骤生成证书集合的二进制表示。在第一步骤中，生成具有第一随机水平的第一表示。第一随机水平对应于相对于均匀分布的第一偏差水平。在后续第二步骤中，将此第一表示变换成包括更高随机水平的第二表示。第二随机水平对应于相对于均匀分布的第二偏差水平。相对于均匀分布的第二偏差水平低于相对于均匀分布的第一偏差水平。换言之，在第二步骤中，从第一表示去除结构或者冗余。在第三步骤中，将第二表示变换成相对于均匀分布具有预定义最大偏差水平的二进制表示。相对于均匀分布的最大偏差水平对应于最小随机水平。

优选地，第一表示和第二表示是非二进制表示。借助第三步骤，可以将这些非二进制表示转换成二进制表示。

根据本发明第一方面的一个实施例，将证书集合划分成用于二进制转换的单位，其中以如下方式来选择用于二进制转换的单位，即，没有代表证书符号的二进制表示的比例小于预定义比例。

借助强力攻击，攻击方仅能排除没有代表有效证书符号的试探解密。因此，限制此类表示的比例降低了受强力攻击影响的程度。作为示例，预定义比例可以设置成1%，这意味着所选的用于二进制转换的单位的二进制表示的至多1%没有代表有效证书符号。本发明



的其它示例实施例可以例如使用预定义比例值 0.01%、0.0001% 或者 5%。

根据本发明第一方面的一个实施例，证书集合划分成各自包括两个或者更多证书符号的用于二进制转换的单位。

使用包括两个或者更多证书符号的用于二进制转换的单位提高了灵活性并且增加了单位的可能数目。这使得更有机会选择没有引入冗余或者引入很少冗余的、用于二进制转换的良好或者最优单位。如果证书集合是 TAN 列表，则例如 3 个或者 6 个十进制数可以建立用于二进制转换的单位。

根据本发明第一方面的一个实施例，第一信道是非信任信道，而第二信道是受信任信道。

将非信任信道理解为证书用户/或证书签发方不信任的信道。非信任信道易受中间攻击方的影响。将受信任信道理解为证书用户和证书签发方信任的信道。

根据本发明第一方面的一个实施例，证书是一次性认证码。此类一次性认证码可以例如是用于在线银行交易的 TAN。

根据本发明第一方面的一个实施例，第一信道是无线通信信道，而第二信道包括安全的因特网连接、电话线和邮件服务之一。

此类信道遍布广泛并且允许该方法的广泛使用。

根据本发明第一方面的一个实施例，用户设备包括移动电话和个人数字助理之一。

此类设备遍布广泛并且允许该方法的广泛使用。

根据本发明的一个实施例，用户设备是受信任设备。将受信任设备理解为证书用户信任的设备。优选地，受信任设备由证书用户拥有和/或控制。优选地，证书签发方也信任受信任设备。

根据本发明的一个实施例，将具有均匀分布的二进制表示限定为其中二进制值 1 和 0 概率相等的分布。

根据本发明的第二方面，提供一种用于将证书集合从证书签发方分发给证书用户的方法，其中证书用户具有用户设备，其中提供

第一信道和第二信道用于用户设备与证书签发方之间的通信，其中该方法在证书服务器中包括步骤：

- 生成共享密钥并且将共享密钥分发给用户设备，或者经由第二信道从用户设备接收共享密钥，
- 生成相对于均匀分布具有预定义最大偏差水平的证书集合的二进制表示，
- 借助共享密钥来加密证书集合的二进制表示，
- 经由第一信道将加密的证书集合分发给用户设备。

本发明的这一方面涉及由证书服务器执行的方法步骤。

根据本发明的第三方面，提供一种包括指令的计算程序，这些指令用于在所述计算机程序在计算机系统上执行时实现根据本发明第二方面的方法的步骤。

计算机系统可以由证书服务器建立。

根据本发明的第四方面，提供一种用于用户设备从证书服务器接收证书集合的方法，其中提供第一信道和第二信道以用于用户设备与证书服务器之间的通信，其中该方法在用户设备中包括步骤：

- 生成共享密钥并且将共享密钥分发给证书服务器，或者经由第二信道从证书服务器接收共享密钥，
- 接收相对于均匀分布具有预定义最大偏差水平的证书集合的二进制表示，其中借助共享密钥来加密证书集合的二进制表示，
- 借助共享密钥对加密的证书集合进行解密，
- 存储解密的证书集合。

本发明的这一方面涉及由用户设备执行的方法步骤。

根据本发明的第五方面，提供一种包括指令的计算程序，这些指令用于在所述计算机程序在计算机系统上执行时实现根据本发明第四方面的方法的步骤。

计算机系统可以由用户设备建立。

根据本发明的第六方面，提供一种用于经由非信任信道将证书集合从证书签发方安全地发送到证书用户的方法，该方法包括步骤：

- 生成相对于均匀分布具有预定义最大偏差水平的对证书集合的二进制表示，
- 借助共享密钥来加密证书集合的二进制表示，
- 经由非信任信道将加密的证书集合从证书签发方发送到证书用户。

本发明的这一方面涉及一种用于经由非信任信道将证书集合从证书签发方安全地发送到证书用户的方法。对共享密钥的分发不是本发明这一方面的主题内容。假设：证书签发方和证书用户拥有共享密钥。

根据本发明的第七方面，提供一种包括指令的计算程序，这些指令用于在所述计算机程序在计算机系统上执行时实现根据本发明第六方面的方法的步骤。

计算机系统可以由证书签发方的证书服务器建立。

根据本发明的另一方面，提供一种用于将证书集合从证书签发方分发给证书用户的系统，其中证书用户具有用户设备，其中提供第一信道和第二信道以用于用户设备与证书签发方之间的通信，提供该系统用于：

- 借助第二信道在用户设备与证书签发方之间分发共享密钥，
- 生成相对于均匀分布具有预定义最大偏差水平的证书集合的二进制表示，
- 借助共享密钥来加密证书集合的二进制表示，
- 经由第一信道将加密的证书集合从证书签发方分发给用户设备，
- 用户设备借助共享密钥对加密的证书集合进行解密。

根据本发明的另一方面，提供一种用于将证书集合分发给证书用户的证书服务器，其中证书用户具有用户设备，其中提供第一信道和第二信道以用于用户设备与证书服务器之间的通信，提供该证书服务器用于：

- 生成共享密钥并且将共享密钥分发给用户设备或者经由第二

信道从用户设备接收共享密钥，

- 生成相对于均匀分布有预定义最大偏差水平的对证书集合的二进制表示，

- 借助共享密钥来加密证书集合的二进制表示，

- 经由第一信道将加密的证书集合从证书签发方分发给用户设备。

根据本发明的另一方面，提供一种被提供用于从证书服务器接收证书集合的用户设备，其中提供第一信道和第二信道以用于用户设备与证书服务器之间的通信，提供该用户设备用于：

- 生成共享密钥并且将共享密钥分发给证书服务器，或者经由第二信道从证书服务器接收共享密钥，

- 接收相对于均匀分布具有预定义最大偏差水平的证书集合的二进制表示，其中证书集合的二进制表示借助共享密钥而加密，

- 借助共享密钥对加密的证书集合进行解密，

- 存储解密的证书集合。

可以按照不同顺序进行本发明不同方面的步骤。另外，也可以组合步骤，即，例如将两个或者更多步骤一起执行。

任何设备特征可以应用于本发明的方法方面，反之亦然。设备特征的优点适用于对应方法特征，反之亦然。

## 附图说明

下文参照以下示意图仅通过示例描述本发明的优选实施例。

附图是仅出于示例目的而提供的并且未必按比例代表本发明的实际示例。在各图中，相同标号用来表示相同或者相似部分。

图 1 是根据本发明一个实施例的系统的框图；

图 2 是该系统的智能卡的框图；

图 3 是该系统的用户设备的框图；

图 4 是该系统的服务器计算机系统的框图；

图 5 是根据本发明一个实施例的另一系统的框图；

- 图 6 是与智能卡相关联的流程图；
- 图 7 是智能卡存储器的框图；
- 图 8 是与服务器计算机系统相关联的流程图；
- 图 9 是与智能卡相关联的另一流程图；
- 图 10 是智能卡存储器的另一框图；
- 图 11 是与智能卡相关联的又一流程图；
- 图 12 是与服务器计算机系统相关联的另一流程图；
- 图 13 是与服务器计算机系统相关联的又一流程图；
- 图 14 是与服务器计算机系统相关联的又一流程图。

### 具体实施方式

图 1 示出了根据本发明一个实施例的系统 100。系统 100 包括用户设备 110。在本发明的这一示例实施例中，用户设备 110 是移动电话。用户设备 110 的其它示例包括个人数字助理（PDA）、有线或者无绳电话或者任何其它用户设备。用户设备 110 包括智能卡 115。

系统 100 包括服务器计算机系统 120，其作为服务器而分配给证书签发方 130。证书签发方 130 可以例如是提供服务的银行、保险公司、网店或者服务实体。提供证书签发方 130 以用于签发证书 145 的集合 140，特别地，是一次性证书的集合。证书 145 可以用作例如访问证书签发方 130 的服务或者与证书签发方 130 的进行交易的验证或者认证手段。证书签发方 130 可以包括多个服务器计算机系统 120，例如，用于生成和分发证书的第一服务器计算机系统 120 和用于验证证书的第二服务器计算机系统。在本发明的这一示例实施例中，假设：一个示出的服务器计算机系统 120 执行证书 145 的生成、分发和验证。根据本发明的一个实施例，证书 145 的集合 140 是交易号（TAN）列表。TAN 列表的每个 TAN 表示证书 145，而 TAN 列表表示证书 145 的集合 140。

建立第一信道 150，以用于用户设备 110 与服务器计算机系统

120之间的通信。第一信道150包括通信网络基础结构155。通信网络基础结构155可以是无线接入网，例如GSM网络之类的移动电话网络。

建立第二信道160，以用于用户设备110与服务器计算机系统120之间的通信。根据本发明这一实施例的第二信道160包括客户端计算机系统170，其作为可连接到服务器计算机系统120的又一设备。客户端计算机系统170包括显示器176、计算机177和作为人工用户接口的键盘175。根据本发明的其它实施例，该又一设备可以是个人数字助理(PDA)、有线或者无绳电话或者移动电话。客户端计算机系统170可以借助通信网络基础结构180来与服务器计算机系统120通信。特别地，通信网络基础结构180可以是因特网。特别地，通信网络基础结构180可以是安全或者受信任因特网连接，例如SSL连接。根据本发明的其它实施例，通信网络基础结构180可以包括无线接入网络(例如移动电话网络)或者有线电话网络。

用户设备110和客户端计算机系统170被分配给证书用户190。证书用户190可以是想要使用证书145来进行交易或者访问证书签发方130的服务的个人或者实体。

提供证书用户190的人工用户交互，以用于客户端计算机系统170与用户设备110之间的通信。该人工用户交互是第二信道160的一部分。根据图1的实施例，第二信道160具有用户设备110的形式为小键盘340的人工用户接口。另外，用户设备110包括显示器330。

为了将信息从客户端计算机系统170传送到用户设备110，可以在客户端计算机系统170的显示器176上显示相应信息。证书用户190读取显示器176上的显示信息，并且借助小键盘340将信息录入到用户设备110中。为了将信息从用户设备110传送到客户端计算机系统170，可以在用户设备110的显示器330上显示相应信息。证书用户190读取显示器330上的显示信息，并且借助小键盘175将信息录入到客户端计算机系统170中。

提供系统 100 以用于将证书 145 的集合 140 从证书签发方 130 分发给证书用户 190。提供第二信道 160 以用于在用户设备 110 与证书签发方 130 之间分发共享密钥 K。特别地，共享密钥 K 为弱密钥。对共享密钥 K 的这分发为证书用户 190 与证书签发方 130 之间的证书分发提供了初始设置。

根据本发明的一个实施例，共享密钥 K 由证书签发方 130 的服务器计算机系统 120 生成。继而，共享密钥 K 经由通信网络基础结构 180 从服务器计算机系统 120 发送到客户端计算机系统 170。继而，共享密钥显示于客户端计算机系统 170 的显示器 176 上，由证书用户 190 读取，并且由证书用户 190 经由小键盘 340 人工录入到用户设备 110 中。由于共享密钥 K 可以是弱密钥并且因此是短密钥，所以可以借助小键盘 340 来辅助其录入。

根据本发明的另一实施例，共享密钥 K 由用户设备 110 生成。继而，共享密钥 K 显示于用户设备 110 的显示器 330 上，由证书用户 190 读取，并且由证书用户 190 借助键盘 175 人工录入到客户端计算机系统 170 中。继而，共享密钥 K 经由通信网络基础结构 180 从客户端计算机系统 170 发送到服务器计算机系统 120。

由于共享密钥 K 可以是弱密钥并且因此是短密钥，所以可以在显示器 330 上便利地读取它，并且借助键盘 175 来辅助其录入。

作为上述两个实施例的结果，证书签发方 130 和证书用户 190 具有共享密钥 K，并且可以将该共享密钥 K 用于经由第一信道 150 来交换加密的信息（特别地，交换加密的证书）。

提供服务器计算机系统 120 以用于生成相对于均匀分布具有预定义最大偏差水平的、证书 145 的集合 140 的二进制表示。提供服务器计算机系统 120 还用于借助共享密钥 K 来加密相对于均匀分布具有预定义最大偏差水平的该二进制表示。继而，证书 145 的加密集合 140 经由第一信道 150 从服务器计算机系统 120 发送到用户设备 110。在用户设备 110 中，证书 145 的加密集合 140 借助共享密钥 K 来解密，并且存储于用户设备 110 中、（特别地，存储在智能

卡 115 中)。

图 2 较为具体地示出了用户设备 110 的智能卡 115。

智能卡 115 包括全部经由总线子系统 240 来互连的存储器 200、中央处理单元 (CPU) 210、加密引擎 220 和输入/输出 (I/O) 子系统 230。在存储器 200 中存储可由 CPU 210 执行的计算机程序码。计算机程序码包括形式为 Java 兼容操作平台的操作系统 250 和工具包 260。工具包 260 建立形式为 Java 小程序 (Applet) 的应用软件。存储器 200 还有助于以防篡改的方式来存储证书 145 的集合 140。证书 145 的集合 140 也表示为 SC。操作系统 250 配置 CPU 210 以执行工具包 260。工具包 260 有助于处理证书集合 140 中的证书 145。随后将具体地描述工具包 260 的功能方面。加密引擎 220 包括密码处理逻辑, 其用于加密和解密将从智能卡 115 发送和由智能卡 115 接收的数据。可以用硬件、软件或者组合硬件和软件来实施密码处理逻辑。

图 3 较为具体地示出了用户设备 110。用户设备 110 包括全部由总线子系统 350 互连的具有射频 (RF) 天线 310 的 RF 级 300、控制逻辑 320、可视显示器 330 和小键盘 340。智能卡 115 可拆卸地插入到用户设备 110 中, 并且智能卡 115 的 I/O 子系统 230 可释放地连接到用户设备 110 的总线子系统 350。在操作中, RF 级 300 和 RF 天线 310 促进用户设备 110 与连接到第一信道 150 的其它设备之间的无线通信。可视显示器 330 在用户与用户设备 110 之间提供图形用户界面, 以用于例如准备消息和读取消息之类的功能。小键盘 340 为用户提供对用户设备 110 的键盘控制, 以用于诸如数据录入和呼叫处理的功能。控制逻辑 320 基于例如从小键盘 340 接收的输入来控制用户设备 110 的功能, 例如呼叫处理。用户设备 110 的输出也由控制逻辑 320 控制, 例如在可视显示器 330 上的数据显示或者经由 RF 级 300 的传出呼叫。类似地, 控制逻辑 320 协调经由总线子系统 350 的、来自智能卡 115 和用户设备 110 的其它单元的数据传送。可以用专用硬件、编程的 CPU 或者专用硬件与编程的 CPU 的组合来



实施控制逻辑 320。

图 4 较为具体地示出了服务器计算机系统 120。服务器计算机系统 120 包括全部由总线子系统 430 互连的存储器 400、CPU 410 和 I/O 子系统 420。在存储器 400 中存储可由 CPU 410 执行的计算机程序码。计算机程序码包括操作系统 440 和证书服务应用软件 (CSAS) 450。操作系统 440 配置 CPU 410 以执行证书服务应用软件 450。证书服务应用软件 450 促进处理证书 145 的集合 140。随后将具体地描述证书服务应用软件 450 的功能方面。

在操作中, 在用户设备 110 与服务计算机系统 120 之间建立第一信道 150。第一信道 150 促进将证书 145 的集合 140 从服务器计算机系统 120 中的证书服务应用软件 450 传送到用户设备 110 中的智能卡 115。在为用户配置智能卡 115 期间, 可以将工具包 260 加载到用户设备 110 的存储器 200 中。备选地, 工具包可以经由第一信道 150 加载到存储器 200 中, 并且被动态刷新。对存储器 200 中的工具包 260 的访问由证书用户 190 经由用户设备 110 设置的 PIN 来加以保护。小键盘 340 可以用于这一目的。备选地, 如果用户设备 110 具有语音识别, 则可以口头设置和重置 PIN。其它设备可以支持甚至更多的数据录入手段。

图 5 示出了根据本发明另一实施例的系统 500。系统 500 的第一信道 150 按照与参照图 1 所示相同的方式来实施。因此将相同的标号用于第一信道 150 的单元。第二信道 520 按照不同于图 1 的第二信道 160 的方式来实施。第二信道 520 包括纸介邮件系统。可以例如经由传统邮政系统来提供纸介邮件。纸介邮件包含将在证书签发方 130 与证书用户 190 之间分发的共享密钥 K。共享密钥 K 分别由证书签发方 130 或者服务器计算机系统 120 生成。其继而通过纸介邮件发送到证书用户 190。提供证书用户 190 以用于开启纸介邮件、读取共享密钥 K 并且借助小键盘 340 将共享密钥 K 人工录入到用户设备 110 中。

下文参照图 6 较为具体地说明用于对共享密钥 K 的初始生成

和分发以及激活智能卡 115 的工具包 260 的流程图。图 6 的流程图基于如上文参照图 1 描述的系统 100。

在步骤 610 中，服务器计算机系统 120 生成共享密钥 K 和证书用户标识码 ID。提供证书用户标识码 ID 以用于标识相应的证书用户 190，并且用于将证书 145 的集合 140 和生成的共享密钥 K 分配给对应证书用户 190。

在步骤 620 中，经由通信网络基础结构 180 将共享密钥 K 和对应证书用户标识码 ID 发送到客户端计算机系统 170。在步骤 630 中，在客户端计算机系统 170 的显示器 176 上显示共享密钥 K 和证书用户标识码 ID。

在步骤 640 中，证书用户 190 经由小键盘 340 录入 PIN。在收到 PIN 时，工具包 260 请求证书用户 190 录入共享密钥 K 和证书用户标识码 ID。在步骤 650 中，证书用户 190 经由小键盘 340 录入共享密钥 K 和证书用户标识码 ID。同样，如果用户设备 110 具有语音识别，则可以口头录入此数据。然而，将会理解，这是一种安全性较低的录入技术，因为用户可能在口述数据时被窃听。在收到上述列举的用户录入时，工具包 260 在步骤 660 中将包含证书用户标识码 ID 的初始化消息（例如 SMS 消息）发送给服务器计算机系统 120 上的证书服务应用软件 450。该认证消息向证书服务应用软件 450 指示已经启用了工具包 260。

参照图 7，智能卡 115 上的存储器 200 现在包含 PIN、共享密钥 K 和证书用户标识码 ID。

参照图 8，当在服务器计算机系统 120 收到初始化消息时，证书服务应用软件 450 在步骤 810 中借助证书用户标识码 ID 来查寻相应的证书用户 190，并且取回为证书用户 190 签发的共享密钥 K。继而，证书服务应用软件 450 在步骤 820 中按照非二进制表示（例如十进制计数制中的 TAN 列表）生成证书 145 的集合 140。在步骤 830 中，生成相对于均匀分布具有预定义最大偏差水平的证书 145 的集合 140 的二进制表示。换言之，将证书 145 的集合 140 的非二进制

表示转换成相对于均匀分布具有预定义最大偏差水平而分布的 0 和 1 的二进制表示。在步骤 840 中，利用共享密钥 K 来加密相对于均匀分布具有预定义最大偏差水平的这一二进制表示。在步骤 850 中，经由第一信道 150 将证书 145 的加密集合 140 从服务器计算机系统 120 发送到用户设备 110。

参照图 9，在步骤 910 中，在用户设备 110 接收证书 145 的加密集合 140。在步骤 920 中，工具包 260 对加密的证书集合进行解密。工具包 260 利用加密引擎 220、借助共享密钥 K 对证书 145 的加密集合 140 进行解密。工具包 360 继而在步骤 930 中将证书 145 的解密集合 140 存储于存储器 200 中。继而完成初始化。参照图 10，存储器 200 现在包含共享密钥 K、PIN、证书用户标识码 ID 和证书 145 的集合 140。

现在参照图 11，当证书用户 190 需要证书 145 以例如进行银行交易时，证书用户 190 在步骤 1110 中再次经由小键盘 340 录入 PIN，从而解锁工具包 260。证书用户 190 继而在步骤 1120 中请求和读取来自工具包 260 的证书 145。取决于证书签发方 130 所使用的证书分配系统，证书 145 可以是证书 145 的集合 140 中的下一证书，或者是特定的证书 145。用户设备 110 在步骤 1140 中在显示器 330 上显示相应证书 145，并且证书用户 190 可以读取这一证书 145 并使用该证书来与证书签发方 130 进行交易。为了向证书用户 190 显示非二进制形式的证书 145，工具包 260 或者用户设备 110 的解码单元将证书 145 的集合 140 的二进制表示重新变换或者重新转换回成非二进制表示。换言之，工具包 260 或者解码单元对证书 145 的集合 140 的二进制表示进行解码。工具包 260 或者用户设备 110 的解码单元具有相应解码工具或者相应解码引擎。

图 12 示出了根据本发明一个实施例的由服务器计算机系统 120 执行的、用于生成证书集合二进制表示的方法的流程图。图 13 示出了证书集合表示的对应示例实施例。

当在服务器计算机系统 120 从用户设备 110 收到初始化消息

时，证书服务应用软件 450 在步骤 1210 中借助证书用户标识码 ID 来查寻相应的证书用户 190，并且取回为相应证书用户 190 签发的共享密钥 K。

在步骤 1220 中，生成集合证书的第一表示。图 13 示出了第一表示 310 的示例。证书集合是 TAN 列表。TAN 列表的第一表示 1310 包括结构化形式的个体 TAN 以及分配。个体 TAN 是有序的并且具有序号。作为示例，第一 TAN 8373 具有序号 01。这一 TAN 列表的结构获得第一随机水平。

在步骤 1230 中，将 TAN 列表的第一表示 1310 变换成 TAN 列表的第二表示 1320。在步骤 1230 中，从第一表示 1310 去除 TAN 列表的结构化形式和分配。这是如下实现的：去除个体 TAN 的序号和结构化分配，并且恰好一个接一个地布置 TAN 而没有中间空间或者结构。第二表示 1320 具有高于第一随机水平的第二随机水平。

在步骤 1240 中，将证书集合的第二表示 1320 变换成相对于均匀分布具有预定义最大偏差水平的二进制表示 1330。

对于步骤 1240，可以使用下文描述的二进制转换或者二进制变换方法之一。

在步骤 1250 中，借助共享密钥 K 来加密相对于均匀分布具有预定义最大偏差水平的二进制表示 1330。这获得加密的证书集合 1340。

在步骤 1260 中，经由第一信道 150 将加密的证书集合从服务器计算机系统 120 发送到用户设备 110。

下文更具体地说明生成相对于均匀分布具有预定义最大偏差水平的证书集合二进制表示的步骤。

一般而言，将要通过第一信道 150 传送的证书集合包括使用字符表 A 构造的一个或者多个字  $w$ （也表示为串  $w$ ）的集合  $W$ 。每个字或者串对应于证书。字符表 A 分别建立证书字符表或者证书字符集合。证书字符表 A 是有限符号集合，其也表示为证书符号。证书符号可以例如是字符或者数字。字  $w$  可以连接字  $w$  以形成消息  $M$ ，

该消息  $M$  是证书字符表  $A$  内的证书符号的序列：

$$\begin{aligned}
 A &= \{a_1, \dots, a_k\} && \text{具有 } k \text{ 个证书符号的证书字符表, } k \geq 1 \\
 w &= s_1 | s_2 | \dots | s_j && \text{通过连接 } j \text{ 个证书符号 } s \text{ 而构造的字, } s \text{ 是} \\
 &&& \text{ } A \text{ 的元素, } j \geq 1; \text{ 每个字代表证书。} \\
 W &= (w_1, \dots, w_q) && q \text{ 个字的集合, } q \geq 1, \text{ 建立证书集合。} \\
 M &= w_1 | \dots | w_q && \text{包含 } n \text{ 个证书符号 } s \text{ 的消息, } s \text{ 是 } A \text{ 的元素,} \\
 &&& n = \sum_{q=1}^q j(w_q)
 \end{aligned}$$

可以不将消息  $M$  视为符号序列，而将其视为基数为  $k$  的数，

例如：

$$M' = s_1 * k^0 + s_2 * k^1 + \dots + s_{(n-1)} * k^{(n-2)} + s_n * k^{(n-1)}$$

为了在加密方案中处理这一消息  $M$  并且为了经由第一信道 150 将其从证书签发方 130 发送到证书用户 190，需要将其转换成二进制表示：

$$M'' = b(1) * 2^0 + b(2) * 2^1 + \dots + b(r-1) * 2^{(r-2)} + b(r) * 2^{(r-1)}$$

其中  $b(i)$  是  $M''$  的位数  $i$ ，而  $r$  是经转换消息的位长度，并且：

$r$  是  $r \geq \ln_2(k^n)$  的最小自然数。

假设  $M'$  中的证书符号  $s(i)$  均匀地分布。也就是说，证书字符表  $A$  中的每个符号  $a(i)$  的出现概率为  $1/k$ 。

如果证书字符表  $A$  不是 2 的幂，则证书集合的二进制表示  $M''$  中的符号 0 和 1 出现的概率为 50%，但是仅仅是针对前最高的  $\ln_2(k)$  位。

对于以下示例，假设：作为证书签发方 130 的银行想要将作为证书列表的交易号 (TAN) 列表托运给证书用户 190。在本例中假定 TAN 具有 6 个十进制数并且假定 TAN 列表包括 100 个 TAN。

将经由第一信道 150 从证书签发方 130 分发给证书用户 190 的证书集合包括 600 个随机十进制数。另外假设，共享密钥  $K$  是 12 位的十进制数。

为了评估该示例的安全水平，假设攻击方窃听证书签发方 130 与证书用户 190 之间经由第一信道 150 的通信。攻击方捕获包含加

密证书集合（即，加密 TAN 列表）的加密消息。现在攻击方可以运行强力攻击来尝试密钥空间中的所有密钥，并且借助所选的测试密钥对已加密的消息进行解密。通过观察加密消息的结构，攻击方可以识别所解密的消息是否是可能的 TAN 列表。如果所选的测试密钥不是正确密钥，则所解密的消息中的数据将是随机的。攻击方可能将其用于排除密钥。

根据本发明的一个实施例，将 TAN 列表视为 600 个十进制数的序列。将 600 个十进制数划分成 200 组 3 个十进制数。这 200 组建立了用于二进制转换的单位。通过应用以下编码或者转换方案来生成 TAN 列表的二进制表示：

借助 10 位的二进制表示(二进制数)对 3 个十进制数的值 0-999 中的每个值进行编码。一般而言，10 位二进制编码方案允许对  $2^{10} = 1024$  个值进行编码。因此，存在一些二进制数（表示），其并未代表已编码的 TAN。这在 TAN 列表的二进制表示中引入了一些冗余或者结构。然而，按照本发明这一实施方式的加密或者转换方案是通过以下方式选择的，即，TAN 列表的二进制表示包括相对于均匀分布的预定义最大偏差水平。证书集合的二进制表示相对于均匀分布的预定义最大偏差水平取决于预定义的安全水平、共享密钥 K 的密钥长度和预定义的验证试探次数。预定义的验证试探次数是证书签发方 130 在其停用或者关闭证书用户 190 的相应账户之前允许的试探次数。

可以如下确定本发明这一示例实施例的安全水平。对加密的 TAN 列表进行解密等同于滚动具有从 0- ( $2^{10}-1$ ) 这些值的 200 个骰子。如果所有骰子仅给出来自 0-999 的值，则测试密钥可能是实际的共享密钥。单个骰子给出 0 与 999 之间有效 TAN 值的可能性是： $P_u = 10^3/2^{10} = 97.66\%$ 。因此，对加密的 TAN 列表利用测试密钥来进行试探解密仅给出有效 TAN 的可能性因此是：

$$P_l = P_u^{100} = 0.871\%$$

这意味着在  $10^{12}$  个可能测试密钥之中，攻击方能够排除所有

候选测试密钥的 99.129%，从而留给他 870 万个可能密钥。如果证书签发方 130 用于错误 TAN 录入的重试计算器的预定义验证试探次数例如是 5，则攻击方命中正确密钥的可能性是 870 万分之 5。这一可能性对应于系统 100 的安全水平。在本例中，可以通过减少预定义验证试探次数、增加共享密钥的密钥长度或者减少 TAN 列表的二进制表示相对于均匀分布的（最大）偏差水平（即增加 TAN 列表的二进制表示的随机水平），来提高安全水平。通过改变这三个参数，证书签发方 130 可以调整和预定义相应应用的安全水平。

根据本发明的另一实施例，将每个个体证书（即在本例中，是包含 6 个十进制数的每个个体 TAN）变换成 20 位的二进制表示。因而，将 600 个十进制数划分成 100 组 6 个十进制数。这 100 组建立了用于本例二进制转换的单位。通过应用以下编码方案来生成 TAN 列表的二进制表示：

将每个 TAN ( $10^6$ ) 编码成 20 位二进制数据。

换言之，借助 20 位的二进制表示（二进制数）对 6 个十进制数的值 0-999999 中的每个值进行编码。一般而言，20 位二进制编码方案允许对  $2^{20} = 1048576$  个值进行编码。因此，同样存在一些二进制数，其并未表示已编码的 TAN。这在 TAN 列表的二进制表示中引入了一些冗余或者结构。

可以如下确定本发明这一示例实施例的安全水平。对加密的 TAN 列表进行解密等同于滚动具有从 0- ( $2^{20}-1$ ) 这些值的 100 个骰子。如果所有骰子都仅给出来自 0-999999 的值，则测试密钥可能是实际的（弱）共享密钥。单个骰子给出 0 与 999999 之间有效 TAN 值的可能性是： $P_u = 10^6/2^{20} = 95.37\%$ 。因此，利用测试密钥对已加密的 TAN 列表进行试探解密仅仅给出有效 TAN 的可能性因此是：

$$P_l = P_u^{100} = 0.871\%$$

这意味着在  $10^{12}$  个可能测试密钥之中，攻击方能够排除所有候选测试密钥的 99.13%，从而留给他 870 万个可能密钥。如果证书签发方用于错误 TAN 录入的重试计算器的预定义验证试探次数例如

是 5，则攻击方命中正确密钥的可能性为 870 万分之 5。这一可能性对应于系统 100 的安全水平。可以通过减少预定验证试探次数、增加弱密钥的密钥长度或者通过减少 TAN 列表的二进制表示相对于均匀分布的（最大）偏差水平，来增加安全水平。通过改变这三个参数，证书签发方 130 可以调整和预定义相应应用的安全水平。

根据本发明的一个实施例，以如下方式来选择安全水平，即强力攻击方命中正确共享密钥的机会小于 1%。

根据本发明的一个实施例，以如下方式来选择安全水平，即强力攻击方命中正确共享密钥的机会小于 0.01%。

根据本发明的一个实施例，以如下方式来选择安全水平，即强力攻击方命中正确共享密钥的机会小于 0.00001%。

如果已经设置这些安全水平之一或者另一安全水平，则可以借助上述方法相应地选择其它参数，即共享密钥的密钥长度、验证试探次数和相对于均匀分布的最大偏差水平。

根据本发明的又一实施例，将 2 个个体证书的群组（即在本例中，为包含 12 个十进制数的两个个体 TAN）变换成 40 位的二进制表示。这 50 个组建立用于二进制转换的单位。因此通过应用以下编码或者转换方案来生成 TAN 列表的二进制表示：

将两个 TAN ( $10^{12}$ ) 这些单位编码成 40 位二进制数据。

换言之，借助 40 位的二进制表示（二进制数）对 12 个十进制数的值 0-999999999999 中的每个值进行编码。一般而言，40 位二进制编码方案允许对  $2^{40} = 1099511627776$  个值进行编码。因此，同样存在一些二进制数，其并未表示已编码的 TAN。这在 TAN 列表的二进制表示中引入了一些冗余或者结构。

可以如下确定本发明这一示例实施例的安全水平。对加密的 TAN 列表进行解密等同于滚动具有从 0- $(2^{40}-1)$  这些值的 50 个骰子。如果所有骰子仅给出来自 0-999999999999 的值，则测试密钥可能是实际的弱共享密钥。单个骰子给出 0 与 999999999999 之间有效 TAN 值的可能性是： $P_u = 10^{12}/2^{40} = 90.95\%$ 。



因此，利用测试密钥对加密的 TAN 列表进行试探解密仅仅给出有效 TAN 的可能性同样是：

$$P_l = P_u^{50} = 0.871\%$$

这意味着在  $10^{12}$  个可能测试密钥之中，攻击方能够排除所有候选测试密钥的 99.13% 从而留给他 870 万个可能密钥。如果证书签发方用于错误 TAN 录入的重试计算器的预定义验证试探次数例如是 5，则攻击方命中正确密钥的可能性为 870 万分之 5。这一可能性对应于证书系统的安全水平。

根据本发明的又一实施例，提供一种为消息 M 提供附加消息空间的编码方案。根据本发明的这一实施例，通过多个附加噪声符号来扩充证书字符表 A。噪声符号是如下符号，它们不是有效的证书符号。扩充的字符表表示为噪声字符表 Ax。噪声字符表 Ax 包括证书字符表 A 的证书符号并且还包含多个噪声符号。优选地，以如下方式来选择多个附加噪声符号的数目，即噪声符号中的符号总数是 2 的幂。

换言之，创建扩展的噪声字符表 Ax，其中：

$$A_x = \{a_1, \dots, a_k, a_{k+1}, \dots, a_{k_x}\}, \text{ 其中 } k < (k_x == 2^x) < 2 * k$$

$a_{k+1}, \dots, a_{k_x}$  是噪声符号，而  $a_1, \dots, a_k$  是证书符号。

作为示例，在 TAN 列表中仅将十进制数视为有效证书符号。这些十进制数由噪声符号 A、B、C、D、E 和 F 扩展。

所得噪声字符表包括证书符号 0、1、2、3、4、5、6、7、8 和 9 以及噪声符号 A、B、C、D、E 和 F。噪声字符表的规模为  $2^4 = 16$  个符号。提供规模与 2 的幂相等的噪声字符表具有的优点在于，证书集合的二进制表示包括 0 和 1 的均匀分布。

图 14 图示了用于生成包括噪声符号的证书集合的二进制表示的方法。

在步骤 1410 中，生成包括预定义数目的证书符号的证书集合。在本例中，同样假设证书集合是 TAN 列表，该 TAN 列表包括作为证书符号的 600 个十进制数。这 600 个十进制数代表 100 个 TAN。

步骤 1410 可以由证书签发方 130 的随机生成器来执行。步骤 1410 的示例输出可以如下：

147462... ..,

其中仅示出 TAN 列表的第一 TAN 147462 而用省略号表示更多的 99 个 TAN。

在步骤 1420 中，生成包含来自噪声字符表的多个伪证书符号和噪声符号的随机消息。伪证书符号的数目大于或者等于证书符号预定义数目。在本例中，证书符号预定义数目是 TAN 列表的规模，即 600。伪证书符号是证书字符表 0、1 的十进制数 0、1、2、3、4、5、6、7、8 和 9。噪声符号由符号 A、B、C、D、E 和 F 建立。随机消息可以由随机十六进制数生成器生成。随机消息在本例中由 960 个十六进制数构成。

步骤 1420 的示例输出可以看起来如下：

A35C9F1ADF86... ..,

其中仅示出随机消息的前 12 个符号而用省略号表示更多的 948 个符号。随机消息的前 12 个符号包括 6 个伪证书符号 (3、5、9、1、8、6) 和 6 个噪声符号 (A、C、F、A、D、F)。

在步骤 1430 中，利用证书符号来替换随机消息的伪证书符号的预定义集合。例如可以将伪证书符号的预定义集合限定为随机消息中的前 600 个伪证书符号。

在本例中，利用证书集合的证书符号 1、4、7、4、6、2 来替换 6 个伪证书符号 3、5、9、1、8、6。

这获得以下消息：

A14C7F4ADF62... ..,

其中同样仅示出消息的前 12 个符号而用点表示更多的 948 个符号。

在步骤 1440 中，借助十六进制编码方案生成此消息的二进制表示。这建立了相对于均匀分布具有预定义最大偏差水平的证书集合的二进制表示。该二进制表示看起来如下：

1010 0001 0100 1100 0111 1111 0100 1010 1101 1111 0110

0010

其中同样仅示出消息的前 12 个符号而用点表示更多的 948 个符号。

可以如下计算本示例与 TAN 列表的全二进制转换相比的规模开销如下：

600 个十进制数 ( $10^{600}$ ) 可以编码在 1994 位中。

上述方案使用 960 个十六进制数，每个都利用 4 位来编码。这获得 3940 位，这是全二进制转换的 193%。

可以如下确定本发明这一示例实施例的安全水平。攻击方仅能排除获得如下解密消息的测试密钥，这些解密消息具有少于 600 个证书符号、即具有 0、1、2、3、4、5、6、7、8 和 9 这些值之一的少于 600 个十六进制数。在本例中的可能性约为 50%。这可以计算如下：

消息包括 960 个十六进制数。假定 10 个证书符号 (0、1、2、3、4、5、6、7、8 和 9) 中的每个符号以相同的概率  $1/16$  出现。因此，在 960 个十六进制数内的证书符号的平均数目是  $10/16 * 960 = 600$ 。换言之，随机消息包括少于 600 个证书符号的概率约为 50%。以 +93% 的附加消息规模为代价达到这一概率。

任何公开的实施例可以与示出和/或描述的一个或者数个其它实施例组合。这对于实施例的一个或者多个特征也是可能的。

#### 附加实施例细节

描述的技术可以实施为方法、装置或者涉及到软件、固件、微代码、硬件和/或其任何组合的制造产品。如这里所用术语“制品”指代在介质中实施的代码或者逻辑，其中这样的介质可以包括硬件逻辑[例如集成电路芯片、可编程门阵列(PGA)、专用集成电路(ASIC)等]或者计算机可读介质如磁存储介质(例如硬盘驱动、软盘、磁带等)、光学存储器(CD-ROM、光盘等)、易失性和非易失性存储器设备[例如电可擦除可编程只读存储器(EEPROM)、只读存储器(ROM)、可编程只读存储器(RPOM)、随机存取存储器(RAM)、

动态随机存取存储器 (DRAM)、静态随机存取存储器 (SRAM)、闪存、固件、可编程逻辑等]。在计算机可读介质中的代码由处理器存取和执行。其中对代码或者逻辑进行编码的介质也可以包括通过空间或者诸如光纤、铜线等传输介质传播的传输信号。的其中对代码或者逻辑进行编码的传输信号还可以包括无线信号、卫星传输、无线电波、红外线信号、蓝牙等。其中对代码或者逻辑进行编码的传输信号能够由发送站发送而由接收站接收，其中可以在接收和发送站或者设备中对在传输信号中编码的代码或者逻辑进行解码并且存储于硬件或者计算机可读介质中。此外，“制造产品”可以包括其中对代码进行实施、处理和执行的硬件和软件部件的组合。当然，本领域技术人员将认识到可以进行许多修改而不脱离实施例的范围并且制造产品可以包括任何信息承载介质。例如，制造产品包括如下存储介质，该存储介质具有存储于其中的指令，这些指令在由机器执行时实现进行操作。

某些实施例可以采用的形式为全硬件实施例、全软件实施例或者既包含硬件单元又包含软件单元的组的实施例。在一个优选实施例中，用软件实施本发明，该软件包括但不限于固件、常驻软件、微代码等。

另外，某些实施例可以采用的形式为可从计算机可用或者计算机可读介质获取的计算机程序产品，该介质提供用于由计算机或者任何指令执行系统使用或者与计算机或者任何指令执行系统结合的程序代码。出于本说明书的目的，计算机可用或者计算机可读介质可以是任何如下装置，该装置可以包含、存储、传达、传播或者传送用于由指令执行系统、装置或者设备使用或者与指令执行系统、装置或者设备结合的程序。该介质可以是电子、磁、光学、电磁、红外线或者半导体系统（或者装置或者设备）或者传播介质。计算机可读介质的示例包括半导体或者固态存储器、磁带、可拆卸计算机盘、随机存取存取 (RAM)、只读存储器 (ROM)、硬磁盘和光盘。光盘的现有示例包括光盘-只读存储器 (CD-ROM)、光盘-读/

写 (CD-R/W) 和 DVD。

措词“某些实施例”、“一个实施例”、“实施例”、“多个实施例”、“该/所述一个实施例”、“该/所述多个实施例”、“一个或者多个实施例”、“一些实施例”、和“一种实施例”除非另有指明则意味着一个或者多个 (但是并非所有) 实施例。措词“包括”、“具有”及其各种变体除非另有指明则意味着“包括但不限于”。项目的列举表除非另有指明, 否则并不意味着任何或者所有项目相互排斥。措词“一个/一种”和“该/所述”除非另有指明, 否则意味着“一个/一种或者多个/多种”。

相互通信的设备除非另有指明则无需相互持续通信。此外, 相互通信的设备可以通过直接地或者通过一个或者多个中介间接地通信。此外, 用数个部件相互通信来描述实施例并不意味着需要所有这样的部件。相反, 描述各种可选部件以说明广泛各种可能实施例。

另外, 虽然可以按照依次顺序描述过程步骤、方法步骤和算法等, 但是可以配置这样的过程、方法和算法以按照替代顺序来工作。换言之, 可以描述的任何步骤序列或者顺序未必表明要求步骤按照该顺序进行。另外, 可以同时、并行或者同期进行一些步骤。

当这里描述单个设备或者产品时, 将清楚可以使用多个设备/产品 (无论它们是否协作) 取代单个设备/产品。类似地, 当这里描述多个设备或者产品 (无论它们是否协作) 时, 将清楚可以使用单个设备/产品取代多个设备或者产品。设备的功能和/或特征可以代之以由并未明确地描述为具有这样的功能/特征的一个或者多个其它设备实施。因此, 其它实施例无需包括设备本身。

在本文中的计算机程序装置或者计算机程序意味着对如下指令的按照任何语言、代码或者符号表示的任何表达, 这些指令用来直接地或者在 a) 转换成另一语言、代码或者符号表示和/或以不同素材形式再现之后使具有信息处理能力的系统执行特定功能。

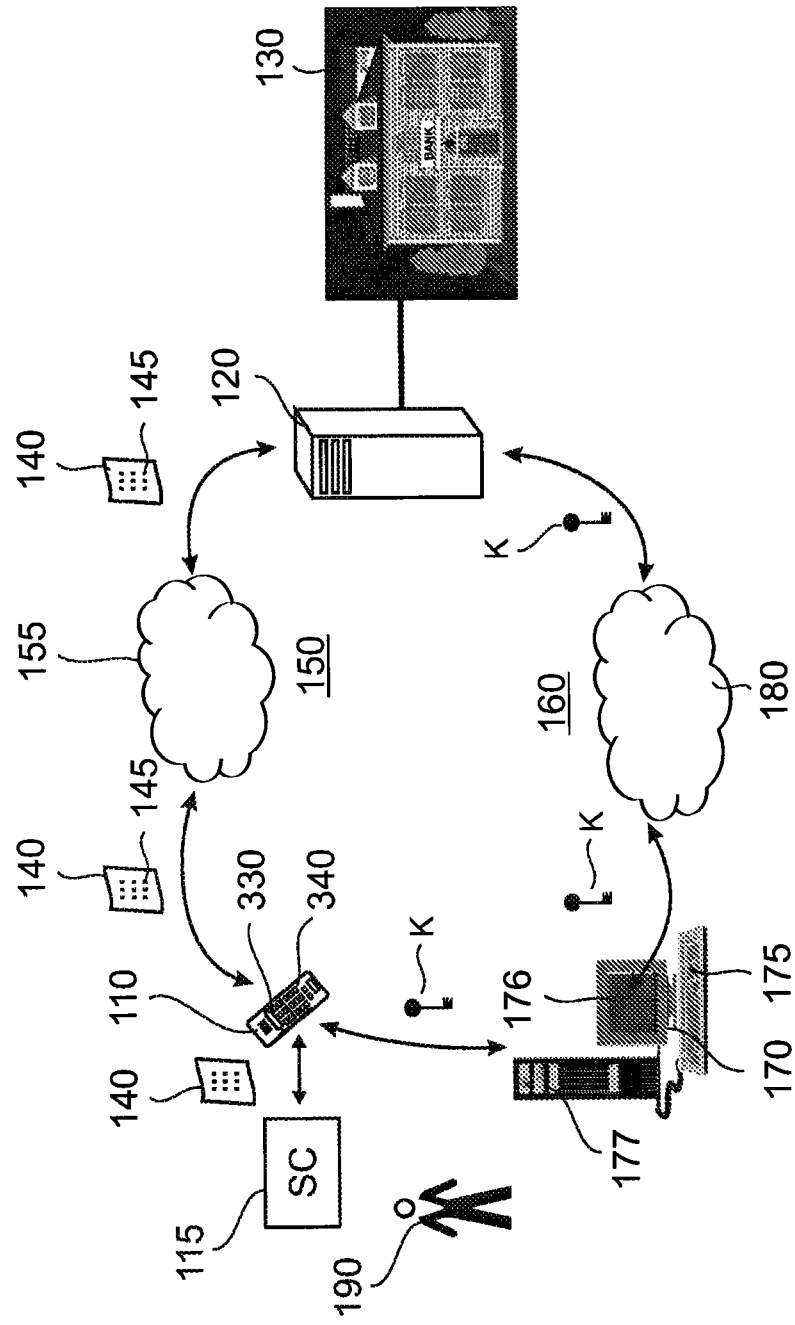


图 1

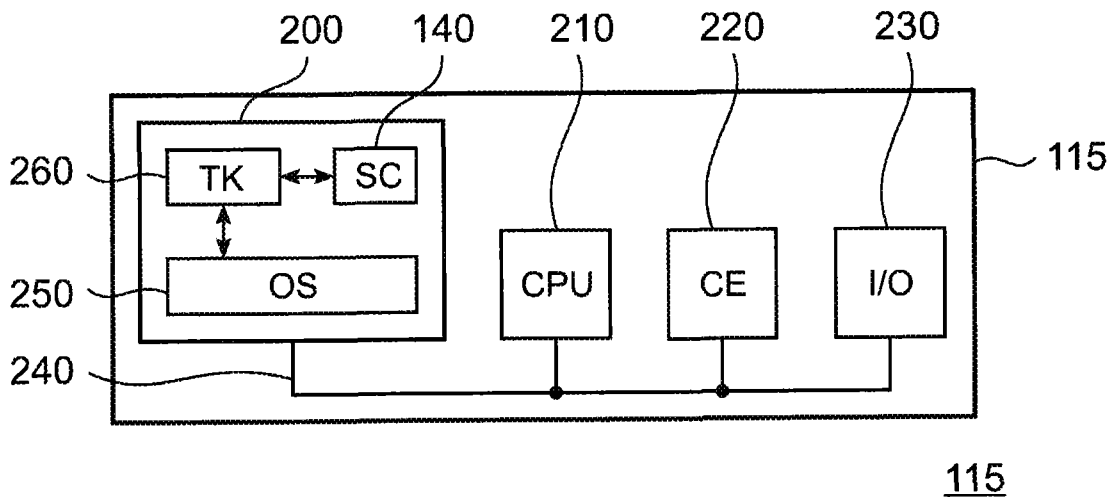


图 2

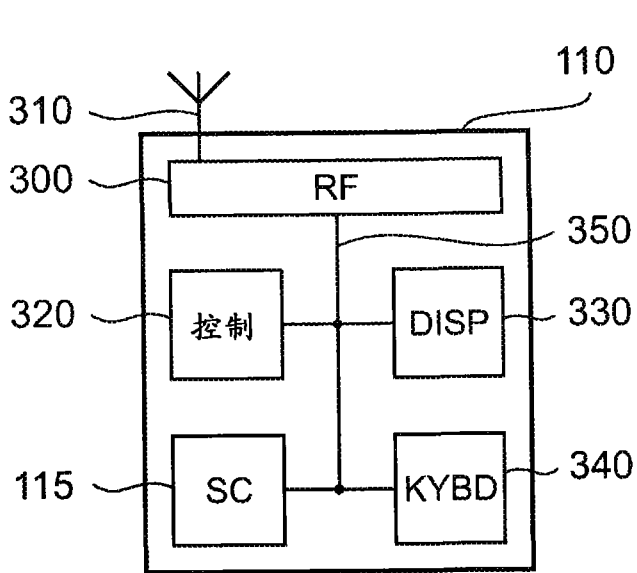


图 3

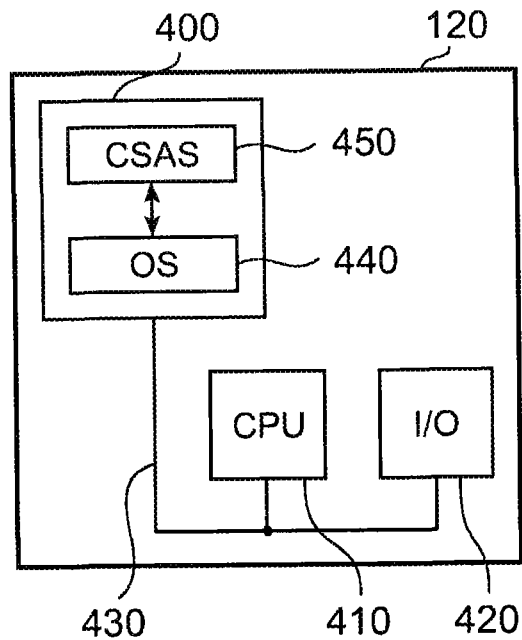


图 4

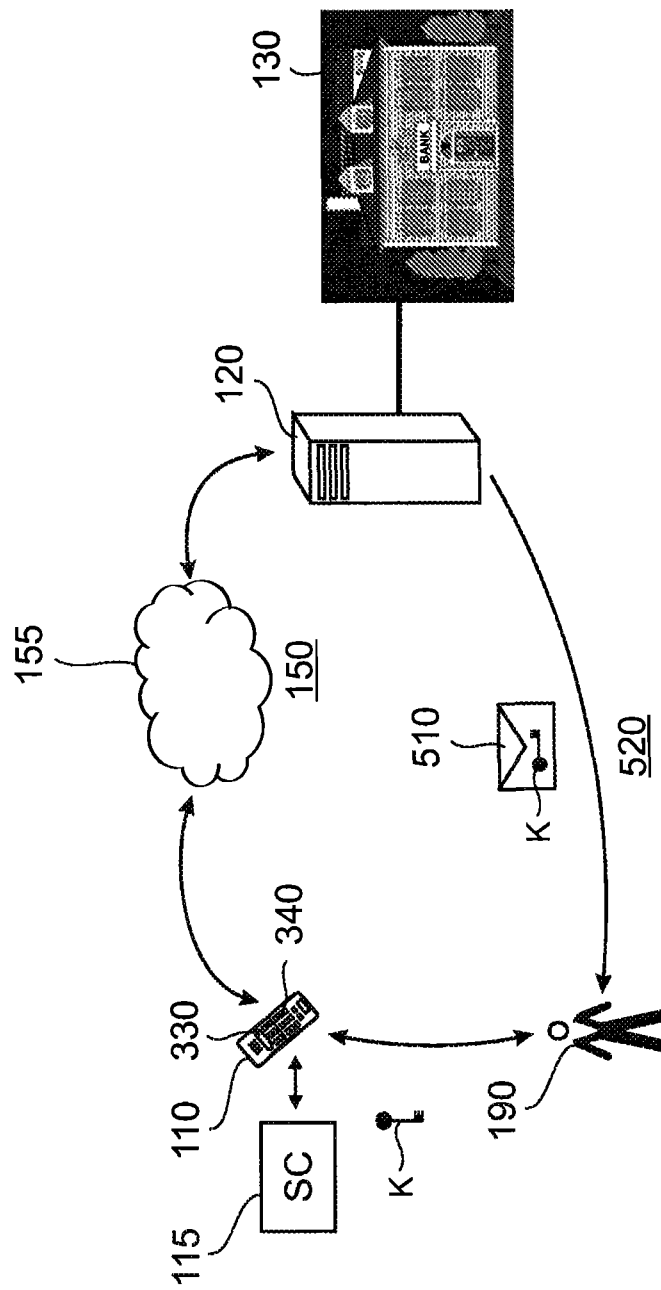


图 5



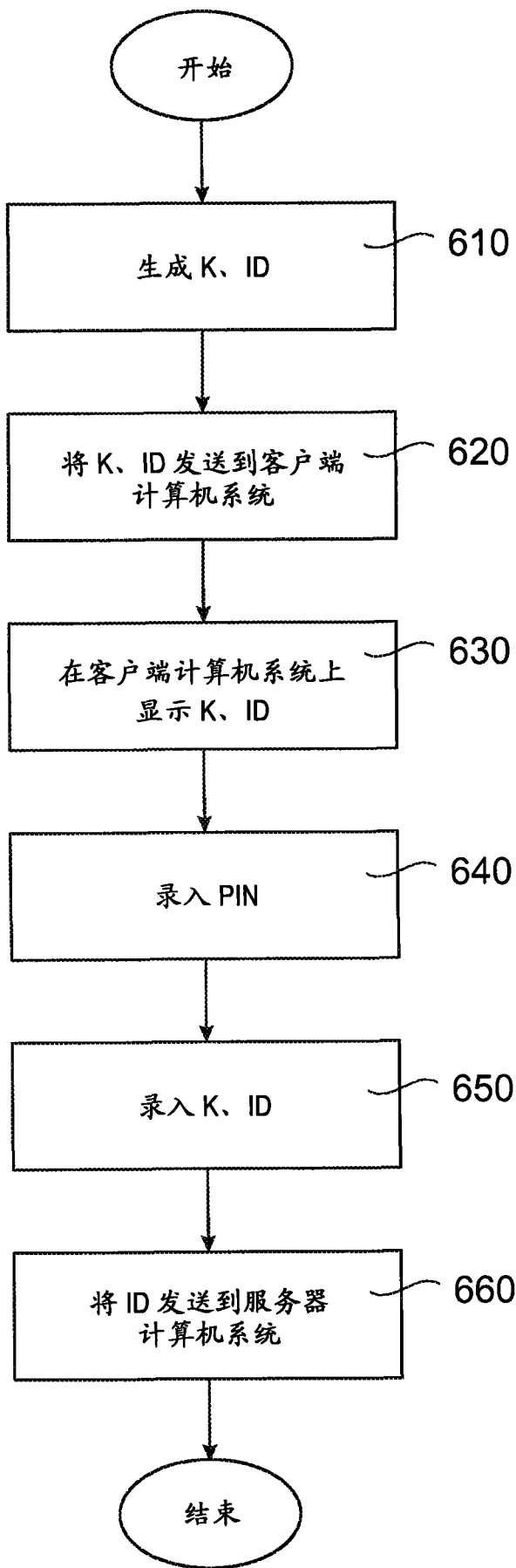


图 6

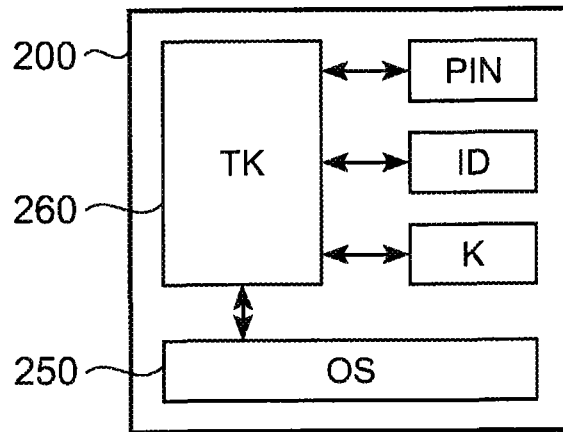


图 7

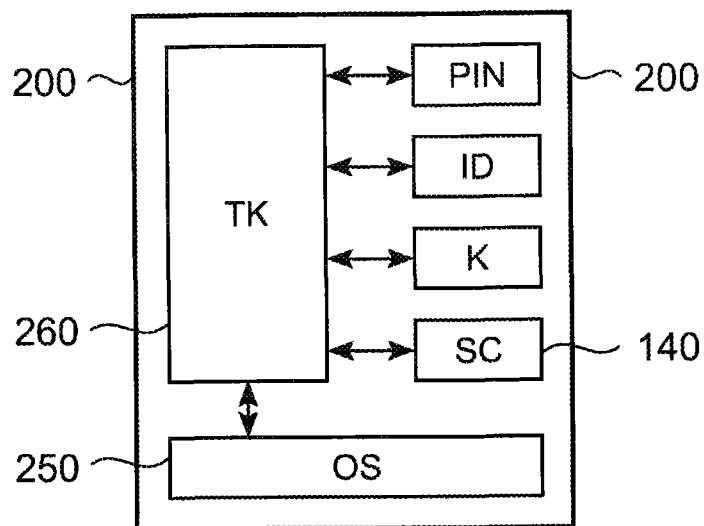


图 10

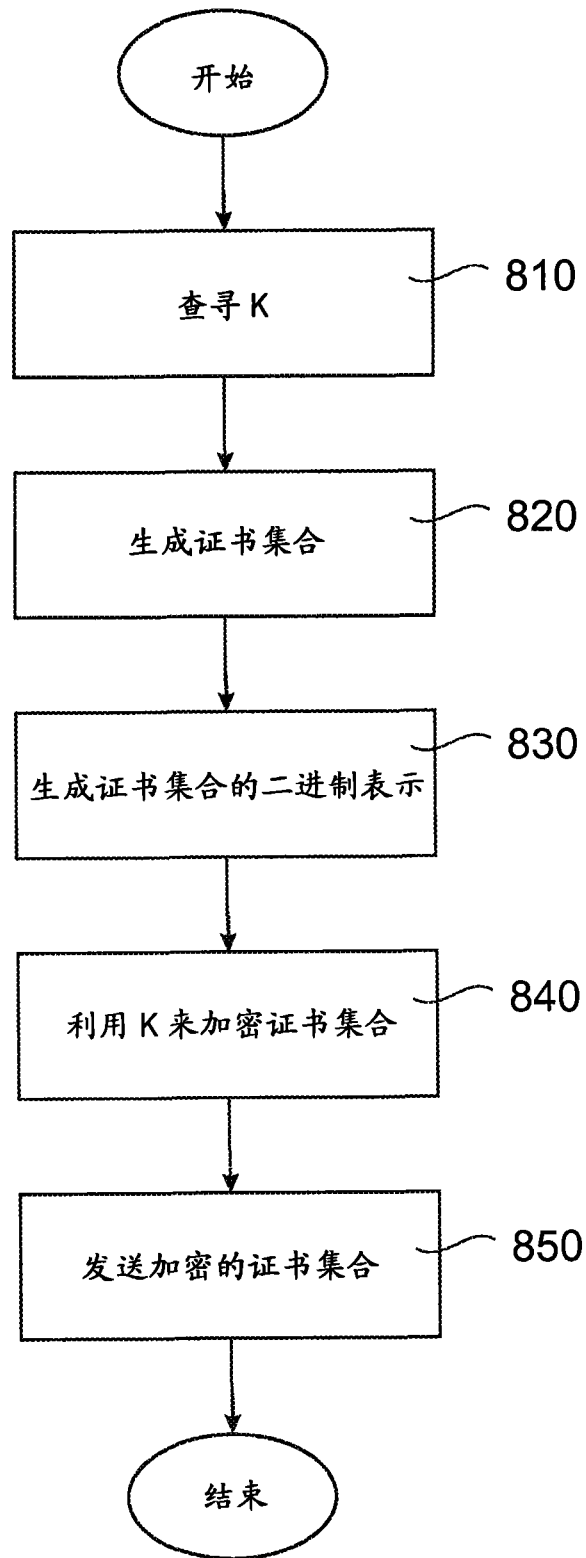


图 8

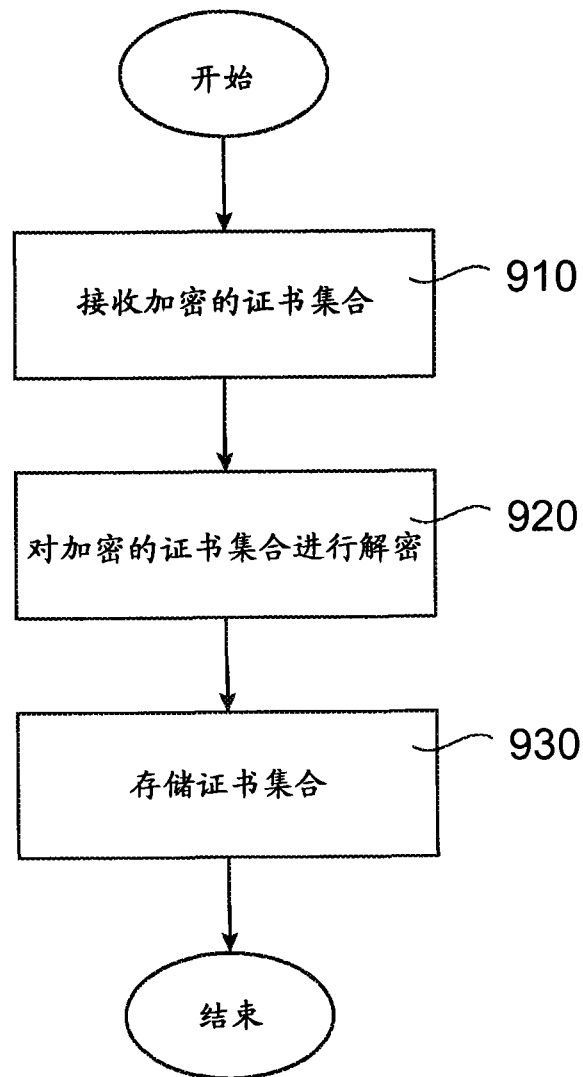


图 9

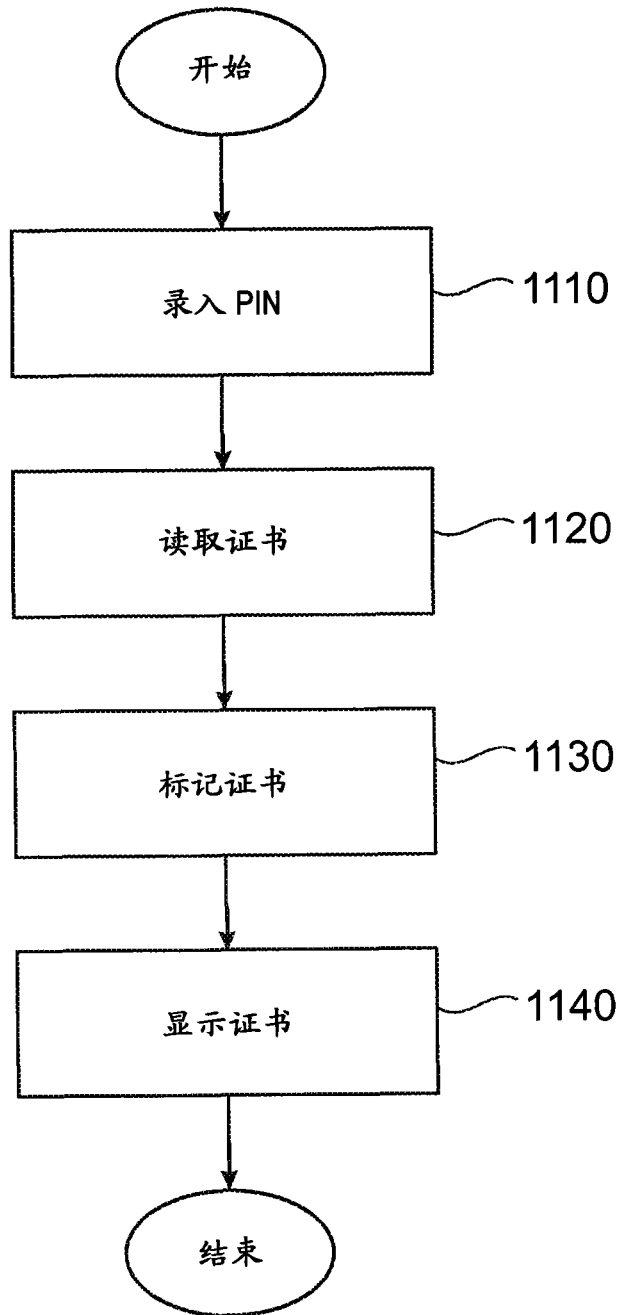


图 11

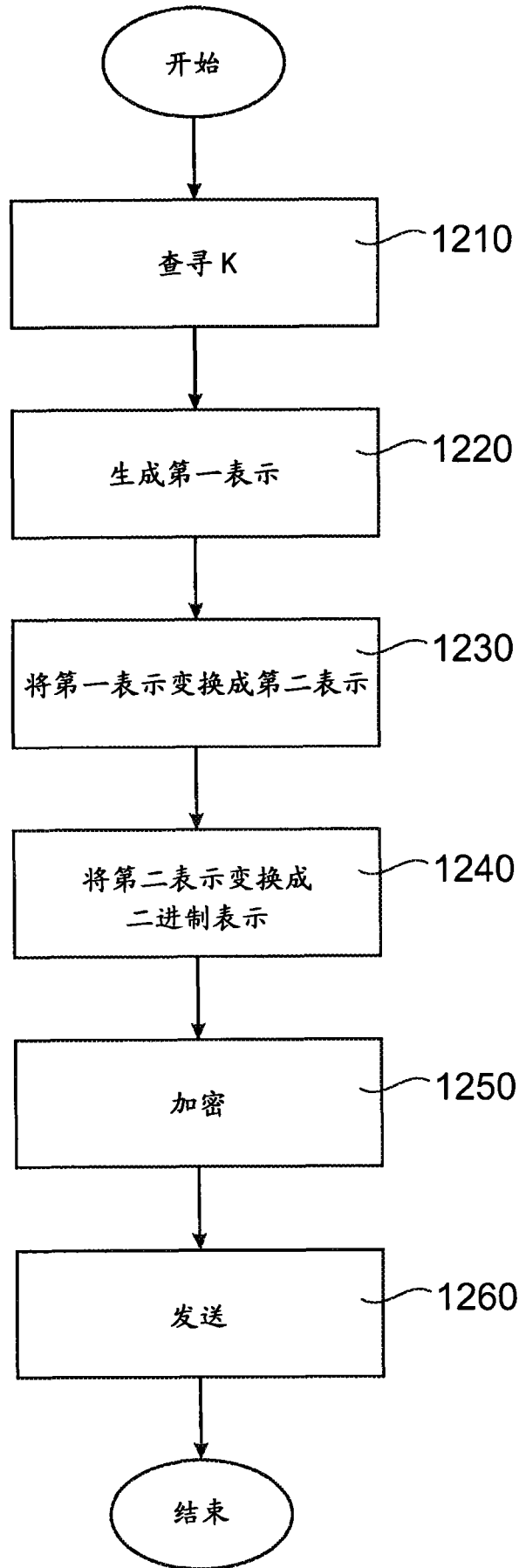


图 12

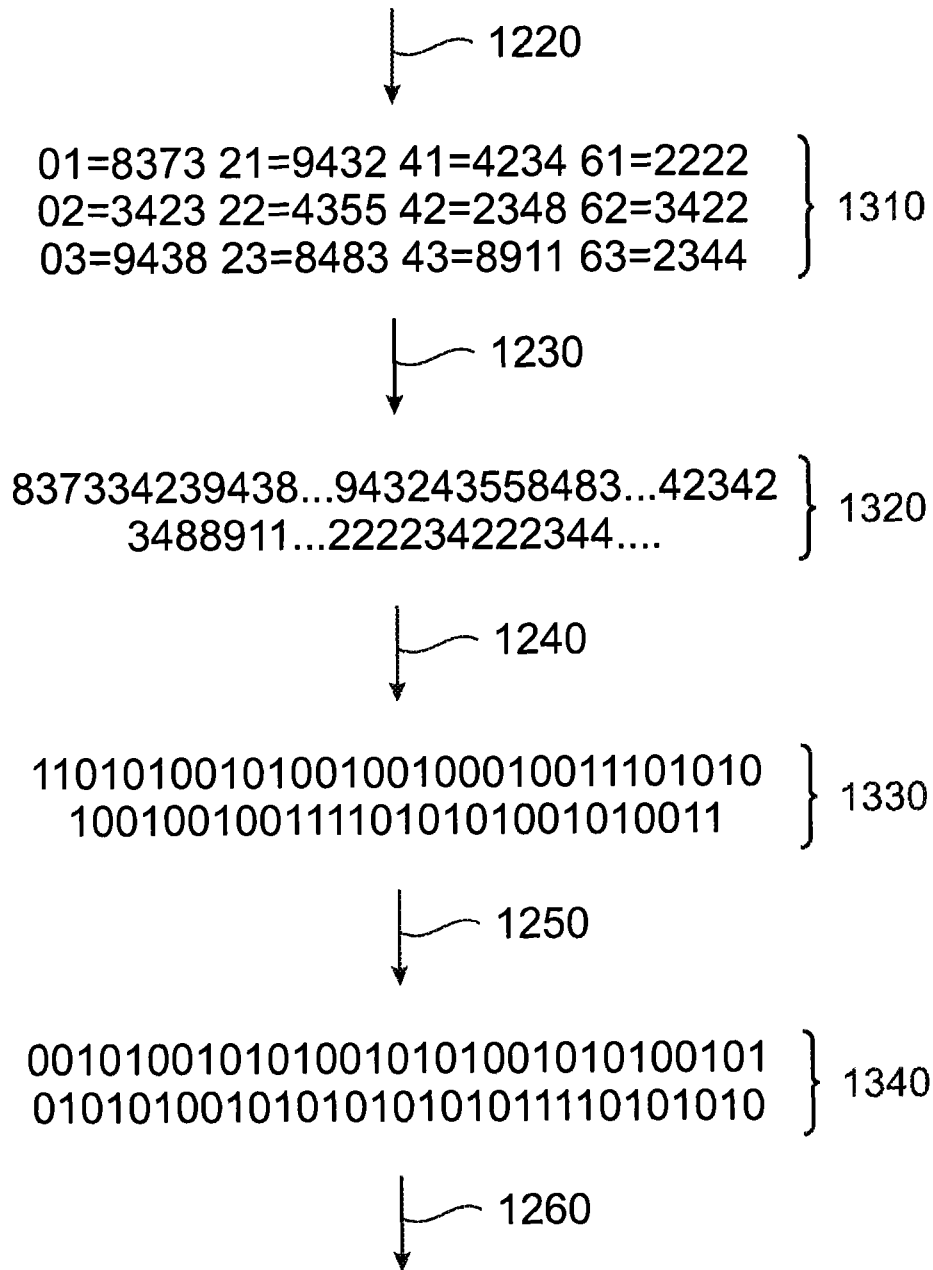


图 13

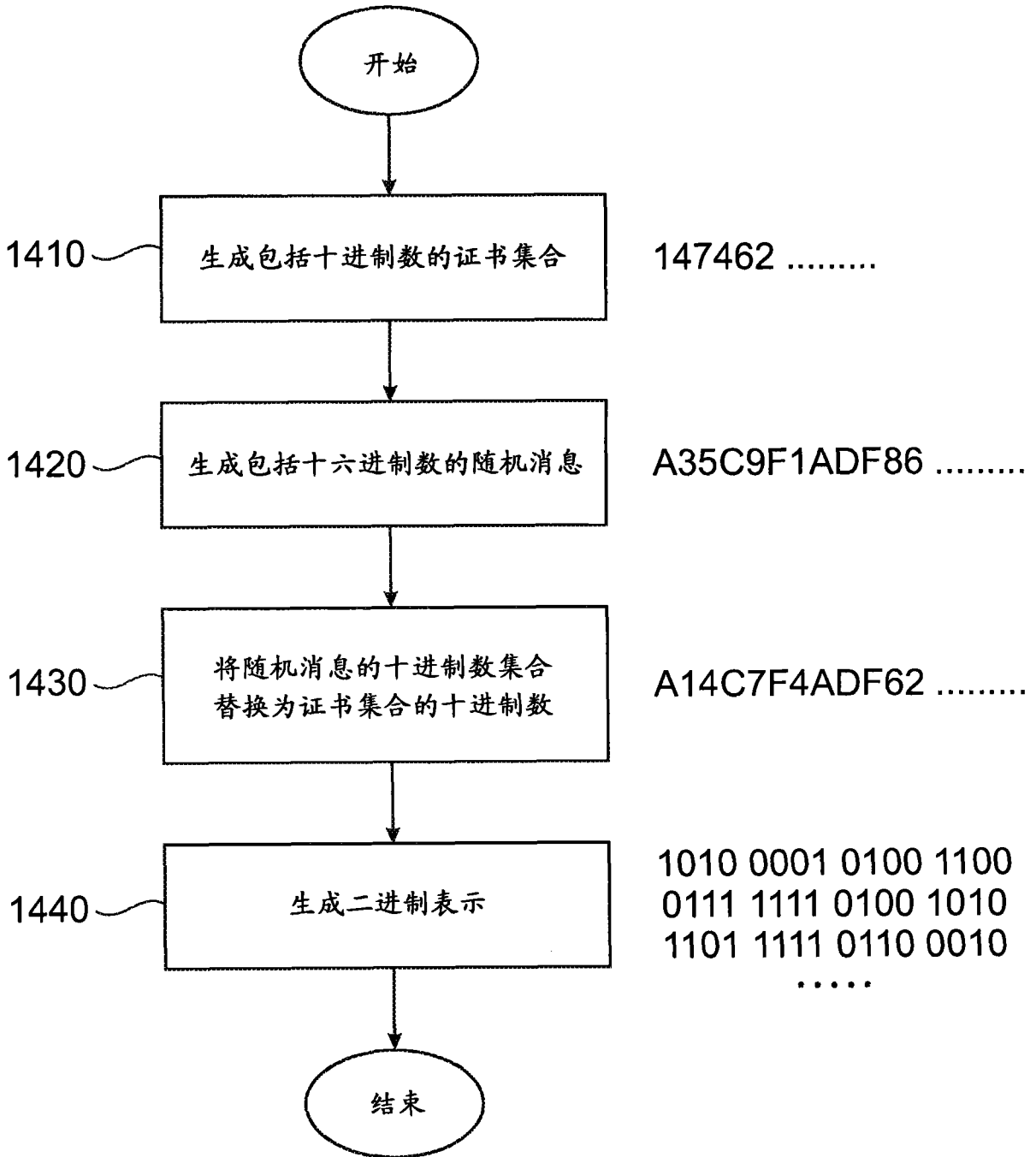


图 14