(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1663171 B
(45)授权公告日 2010.05.05

(21)申请号 03814818.8

(22)申请日 2003.05.15

(30)优先权数据
60/380,652 2002.05.15 US
10/171,960 2002.06.13 US

(85)PCT申请进入国家阶段日
2004.12.24

(86)PCT申请的申请数据
PCT/US2003/015612 2003.05.15

(87)PCT申请的公布数据
WO2003/098865 EN 2003.11.27

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 A·甘特曼

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 钱慰民

(51)Int.Cl.
H04L 9/00(2006.01)
G06F 11/30(2006.01)
H04N 7/167(2006.01)

(56)对比文件
CN 1272934 A,2000.11.08, 全文.
US 6016476 A,2000.01.18, 全文.
US 5787154 A,1998.07.28, 说明书第3栏第22行至第5栏第19行,第6栏第66行至第7栏第22行,第9栏第1行至第15行,图1、5.
US 5491752 A,1996.02.13, 说明书第11栏第56行至第12栏第63行、图5,7.
US 6088450 A,2000.07.11, 全文.

审查员 鲁艳萍

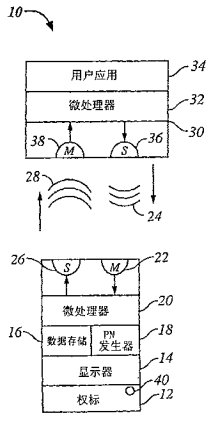
权利要求书 2 页 说明书 4 页 附图 3 页

(54)发明名称

使用声音数字签名发生器作为预言的系统和方法

(57)摘要

一种手持声音权标(12),此权标可用作请求应用的伪随机预言(oracle),所述请求应用能产生被发送至权标的询问。权标(12)的用户可决定是否允许此权标(12)用作预言(oracle),若是,则用户使权标(12)数字地签名该询问并回送至请求应用(34),以便将此数字签名的询问用作加密密钥。加密后,请求应用删除此已签名的询问,在加密过程后随后是解密。



CN 1663171 B

1. 一种加密方法，包括：

产生一个询问；

通过声音信号将此询问发送至便携权标；

决定是否允许权标充当伪随机预言，若是，则使权标对询问进行数字签名以产生一个已签名询问；

通过声音信号发送已签名询问；以及

使用已签名询问来加密数据；

其中所述权标至少部分通过将询问与私有密钥以及伪随机数 PN 相结合来对询问进行数字签名，所述方法还包括：

存储 PN 并当再次收到此询问时重新使用此 PN 对询问进行签名。

2. 如权利要求 1 所述的方法，其中的询问是由一请求应用产生的，所述请求应用使用已签名询问加密数据，并在用完后删除已签名询问。

3. 如权利要求 2 所述的方法，其中所述询问以用户可读形式显示以便于判决动作。

4. 如权利要求 1 所述的方法，其中私有密钥是机密的，并有一对应的公共密钥。

5. 如权利要求 1 所述的方法，其中已签名询问是使用当被给予第一询问时总是给出第一已签名询问的进程来产生的。

6. 一种加密系统，包括：

至少一个请求应用，其使用一无线通信路径将至少一个询问发送到至少一个权标；以及

至少一个权标，其接收询问并使用至少一个私有密钥对所述询问进行数字签名以给出一个已签名询问，权标使用无线通信路径将已签名询问发送至请求应用，请求应用使用此已签名询问来加密数据；

其中权标至少部分地通过将询问与私有密钥和伪随机数 PN 相结合以对询问进行数字签名，权标在对询问签名后存储 PN，并且在再次接收此询问时重新使用此 PN 码对询问进行签名。

7. 如权利要求 6 所述的系统，其中请求应用在加密数据之后删除此已签名询问。

8. 如权利要求 6 所述的系统，其中权标将询问显示给用户以便于用户决定是否允许权标对此询问签名。

9. 如权利要求 6 所述的系统，其中的无线通信路径是声音无线通信路径。

10. 如权利要求 6 所述的系统，其中的已签名询问是使用在被给予第一询问时总是给出第一已签名询问的进程而产生的。

11. 一种加密系统，包括：

接收询问并对询问进行数字签名以产生已签名询问作为响应的权标装置；

将已签名询问发送至请求应用的声音装置；

使用已签名询问对与请求应用相关联的数据进行加密的装置；

其中用于接收和生成的装置至少部分地通过将询问与私有密钥和伪随机数 PN 相结合而对询问进行数字签名；以及

其中所述权标装置进一步用于：当询问被签名时，存储 PN 并当再次收到此询问时重新使用此 PN 对询问进行签名。

12. 如权利要求 11 所述的系统，其中所述权标装置仅仅响应于从用户接收对权标装置产生已签名询问的授权时才产生已签名询问。

13. 如权利要求 11 所述的系统，其中所述权标装置总是响应于询问而产生相同的已签名询问。

14. 如权利要求 11 所述的系统，其中所述权标装置包括手持声音权标。

15. 如权利要求 12 所述的系统，其中所述权标装置进一步地包括用于显示询问的装置。

使用声音数字签名发生器作为预言的系统和方法

[0001] 背景

[0002] 相关申请

[0003] 本申请要求于2002年5月15日提交的，序号为60/380,652，题为“SYSTEM ANDMETHOD FOR USING ACOUSTIC DIGITAL SIGNATURE GENERATOR AS ORACLE（使用声音数字签名发生器作为预言的系统与方法）”的美国专利临时申请的优先权。

[0004] 领域

[0005] 本发明一般涉及伪随机预言（oracle）。

[0006] 背景

[0007] 以上标识的专利申请公开了一种手持的基于声音的“权标”，用户可操控此权标把表示机密信息的声音信号发送至一种称作“认证器”、“检验器”或“接收器”的设备，据此信号认证用户。正如在这些应用中认识到的，基于声音的权标的优越性在于，现有大量已安装的基础设施来接收和发送声音以及从声音导出的电信号。尤其现存的全球电话系统来发送代表声音信息的数据，除了电话以外，通过这一相同系统（如体现在因特网中）互连的许多计算设备现在也拥有麦克风和扬声器（或者可以简单改装来拥有）。

[0008] 正如这里所认识到的，声音权标的优越性在于可以在权标上以防止没有密钥的接收器获取私人信息的方式来发送信息。尤其前文提到的申请公开了使用私有密钥/公共原理数字地签名消息的声音权标。更具体地，声音权标通过将消息与机密信息（私有密钥）以及与伪随机码（PN）结合，来产生已签名的消息，此消息仅能被正在处理这一对应私有密钥的公共密钥的实体认证为可信，从而数字地签名消息。

[0009] 正如这里更进一步认识到的，以上讨论的声音权标的属性使其适于用作加密目的的伪随机预言。更具体地，本发明认为，若应用要求较强的加密密钥，则它选择性地允许此应用通过权标用户来访问权标，以获得权标中机密信息的产物作为加密密钥，而非机密信息本身，从而保证信息的安全。

发明内容

[0010] 公开了一种使用手持声音权标作为伪随机预言实质上将一易记询问转换为一伪随机加密密钥的方法。声音权标所产生的伪随机加密密钥是一较强密钥，未授权方很难破解。

[0011] 据此，加密方法包括产生询问、以及将此询问声学地发送至便携权标。更进一步，此方法包括决定是否允许权标充当伪随机预言，若是，则使权标数字地签名询问以给出一个已签名询问。已签名询问被声学地发送用于加密数据。

[0012] 在一优选的非限定示范例中，询问由使用已签名询问来加密数据的请求应用所产生。若有需要，此询问可以用户可读形式显示，帮助用户决定是否允许此权标被用作伪随机预言。

[0013] 在示例性的非限定性实施例中，权标至少部分地通过将询问与私有密钥相结合而对询问进行数字签名。此私有密钥可以是秘密的并有一对应的公共密钥。

[0014] 若有需要，可使用当被给予同一询问时总能给出相同的已签名询问的进程来产生已签名询问。例如，通过将询问与私有密钥以及伪随机码 (PN) 相结合，权标能对询问进行数字签名。当询问被签名后，可存储PN，以便在第二次收到同一询问（如用于解密目的）时重新使用。

[0015] 另一方面，加密系统包括一请求应用，此应用使用无线通信路径将询问发送至权标。权标接收此询问，并使用私有密钥对此询问数字地签名，并给出一个已签名询问。然后权标使用无线通信路径将此已签名询问发送至请求应用，这样请求应用就可以使用此已签名询问来加密数据。

[0016] 还有一方面，加密系统包括从请求应用发送询问的声音装置、以及接收询问并响应于此而产生已签名询问的装置。系统提供了用于将已签名询问发送至请求应用的声音装置。系统还提供了使用已签名询问对与请求应用相关联的数据进行加密的装置。

[0017] 通过下面提出的结合附图的描述，本发明的细节、结构和操作将变得更加明显，附图中相同的元件具有相同的标识，其中：

附图说明

[0018] 图 1 是本系统的框图；

[0019] 图 2 是加密逻辑的流程图；以及

[0020] 图 3 是解密逻辑的流程图。

具体实施方式

[0021] 首先参考图 1，显示一般由 10 指定的一个系统，包含一可配置为钥匙链或其他小型设备 12 的便携手持权标。然而本发明也可应用于其他权标配置，如移动通信站，包括手提电脑、无线手机或电话、数据收发机、寻呼机、手持或车载定位仪（包括汽车、卡车、船、飞机、火车）。无线通信设备有时也指用户终端、移动站、移动单元、用户单元、移动无线电或无线电话、无线单元，或在某些无线系统中简称为“用户”和“移动设备”。

[0022] 在任何情况下，优选的权标 12 包括视觉显示器 14 和电子数据存储 16。权标 12 也可包括伪随机数 (PN) 发生器 18。权标微处理器 20 访问 PN 发生器 18 及数据存储 16，并使显示器 14 显示用户可读取或接听的字符或图形信息。

[0023] 如图 1 所示，麦克风 22 接收声波 24 并将其转为电子信号，权标微处理器 20 可从麦克风 22 接收电子信号。同样，权标微处理器 20 也可将电子信号发送至扬声器 26，扬声器 26 将其转换为声音信号 28。如下文进一步公开的，接收到的声音信号 24 可能代表一个来自用户组件 30 的询问，如对加密密钥的请求，而发送的声音信号 28 可能代表一个已签名询问，如所请求的加密密钥。虽然声音无线通信是优选的，但是也可以使用其他无线路径，如射频路径。

[0024] 举例来说，用户组件 30 可以是一台电脑，这台电脑包含执行软件实现的用户应用 34 的请求微处理器 32。而用户应用 34 可以是例如字处理应用或其他文档生成应用，或更一般的数据生成应用，这些应用可能希望用较强加密密钥对其生成的数据进行加密。任何情况下，用户组件 30 都可包括扬声器 36 和麦克风 38，扬声器 36 用于发送询问的声音表示，麦克风 38 用于接收应答的声音表示。扬声器 36 与麦克风 38 都与请求微处理器 32 通信。

[0025] 按照本领域已知并且在以下标准中提出的公共密钥 / 私有密钥原理，如 2000 年 1 月出版的美国国家标准与技术协会 (NIST) 联邦信息处理标准出版物第 186-2 号 (National Institute for Standards and Technology(NIST)FederalInformation Processing Standards Publication 186-2) 中所提出，权标 12 内的签名算法（由权标微处理器 20 执行）可将私有密钥与待签名的消息以及 PN 发生器 18 产生的随机数“k”相结合，给出一个随机对 (r,s) 数字签名。最好是，权标微处理器 20 在从一个或多个激活元件 40（例如触发开关、音频激活设备或按钮）处接收激活信号时执行签名算法。需要理解的是，权标微处理器 20 可包含本领域公知的适当的数字处理器、以及必要的时钟、数模转换电路和模数转换电路。

[0026] 权标微处理器 20 访问数据存储 16，这样当使用多个激活元件 40 时，其中的一个或多个可以与存储 16 中的某一私有密钥相关联。按照下面公开的一个非限制性的示范性实施例，除了私有密钥 / 公共密钥对中的一个或多个私有密钥以外，数据存储 16 还可保持公共密钥 ID，若有需要，还有已经生成并用于签名询问的 PN，以及 PN 与询问的相关结果。

[0027] 图 2 示出本发明的加密逻辑。从方块 42 开始，用户应用 34 产生了一个询问（例如一个易记的询问，如单词“password（密码）”），并被从用户组件 30 通过参照图 1 讨论的通信路径发送到权标 12。若有需要，在方块 44 处，权标 12 可以显示询问，并且若有需要，以用户可读形式在显示器 14 上显示询问的来源，这样用户可以在判断菱形 46 处决定是否允许权标 12 充当伪随机预言。若用户决定不允许应用 34 为预言目的而访问权标 12，则此逻辑在状态 48 处结束。

[0028] 另一方面，若用户决定允许权标 12 充当预言，用户可通过操控激活元件 40 来表明这一点。这样逻辑就从判定菱形 46 前进到方块 50，在此权标对询问进行数字签名以给出一个已签名询问。在某优选的非限定性实施例中，权标使用一签名进程，该进程在收到同一询问时总是能给出同样的已签名询问。例如，权标 12 可将询问与数据存储 16 中的私有密钥相结合，但是不与 PN 发生器 18 产生的 PN 相结合。或者遵循常规的私有密钥协议，其中已签名询问是通过将询问与私有密钥及 PN 共同结合而产生的，不过使用的是顺序存放在数据存储 16 中的 PN 码，与之共同存放的是 PN 与所使用的特定询问的相关结果，这样做法的目的将在下文公开。

[0029] 移至方块 52，权标 12 使用上文公开的通信路径将已签名询问发送至用户组件 30，用于将已签名询问作为用户应用 34 的加密密钥来在方块 54 处加密数据，使用如本领域已知的 DES 加密原理。最好是，应用前进至方块 56 并从其内存中、以及从与其上可能已保存已签名询问的用户组件 30 相关联的任何外围存储设备中（如硬盘）删除此已签名询问。

[0030] 在需要解密数据时，则调用图 3 中的逻辑。从方块 58 开始，用户组件 30 将与图 2 中所使用的相同询问发送至权标 12。若有需要，在方块 60 处，权标 12 通过显示器 14 将询问以用户可读形式显示，这样用户可以在判定菱形 62 处决定是否允许权标 12 充当伪随机预言用于解密。若用户不允许，则逻辑在状态 64 处结束。反之若用户允许，则逻辑前进至方块 66，其中权标对询问进行数字签名以产生一个已签名询问。在上述优选的非限定性实施例中，希望当给予同一输入询问时，权标总是产生同样的已签名询问，权标可以使用不需要 PN 的签名程序重新产生与为加密产生的询问相同的已签名询问，或者它可以使用常规的私有密钥协议产生相同的已签名询问，除了以下特例。用于在加密期间产生已签名询问并且

随后被存储在数据存储 16 中（与其和询问的相关结果共同存储）的 PN 可基于此询问在方块 66 处被检取，并与询问及私有密钥相结合，以给出一个已签名询问。

[0031] 移至方块 68，权标 12 将已签名询问发送至用户组件 30，用户应用 34 使用此已签名询问在方块 70 处解密。最好是，应用前进至方块 72 处，从其内存中、以及从与可能已存储着已签名询问的用户组件 30 相关的任何外围存储设备（例如硬盘）中删除此已签名询问。

[0032] 虽然这里所示并详细描述的特定的“使用声音数字签名发生器作为预言的系统和方法”完全能实现本发明的上述目标，可以理解它是本发明当前优选的实施例，因此代表了由本发明宽泛构想的主题，本发明的范围完全包含了对于本领域技术人员显而易见的其它实施例，因此本发明的范围仅受所附权利要求的限制，权利要求中除非特别指明，否则单数的元件不是指“一个且仅有一个”，而是指“一个或多个”。上述优选实施例的元素的所有结构和功能上的等价物都通过引用被结合于此，并且由权利要求所包含，它们对于本领域普通技术人员是已知或者稍后将得知的。此外，设备或方法不必要解决上面由本发明设法解决的每一个问题，因为它被权利要求所包含。此外，本公开内容中的元件、组件或方法步骤都不是专门公开的，无论所述元件、组件或方法步骤是否在权利要求中特别指出。这里没有权利要求元素应被视为在 35U.S.C. §112 第六段的规定下，除非使用短语“用于 ... 的装置”特别指出所述元素，或者在方法权利要求的情况下，用“步骤”而不是“动作”指出该元素。

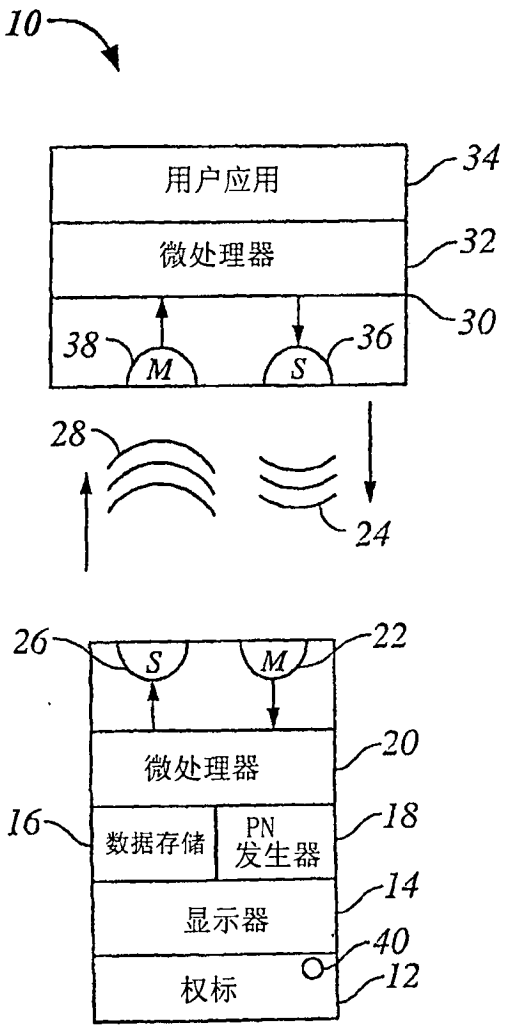

10
用户应用
34
微处理器
32
30
38
M
S
36
28
24
26
S
M
22
微处理器
20
16
数据存储
PN
发生器
18
显示器
14
40
权标
12

图 1

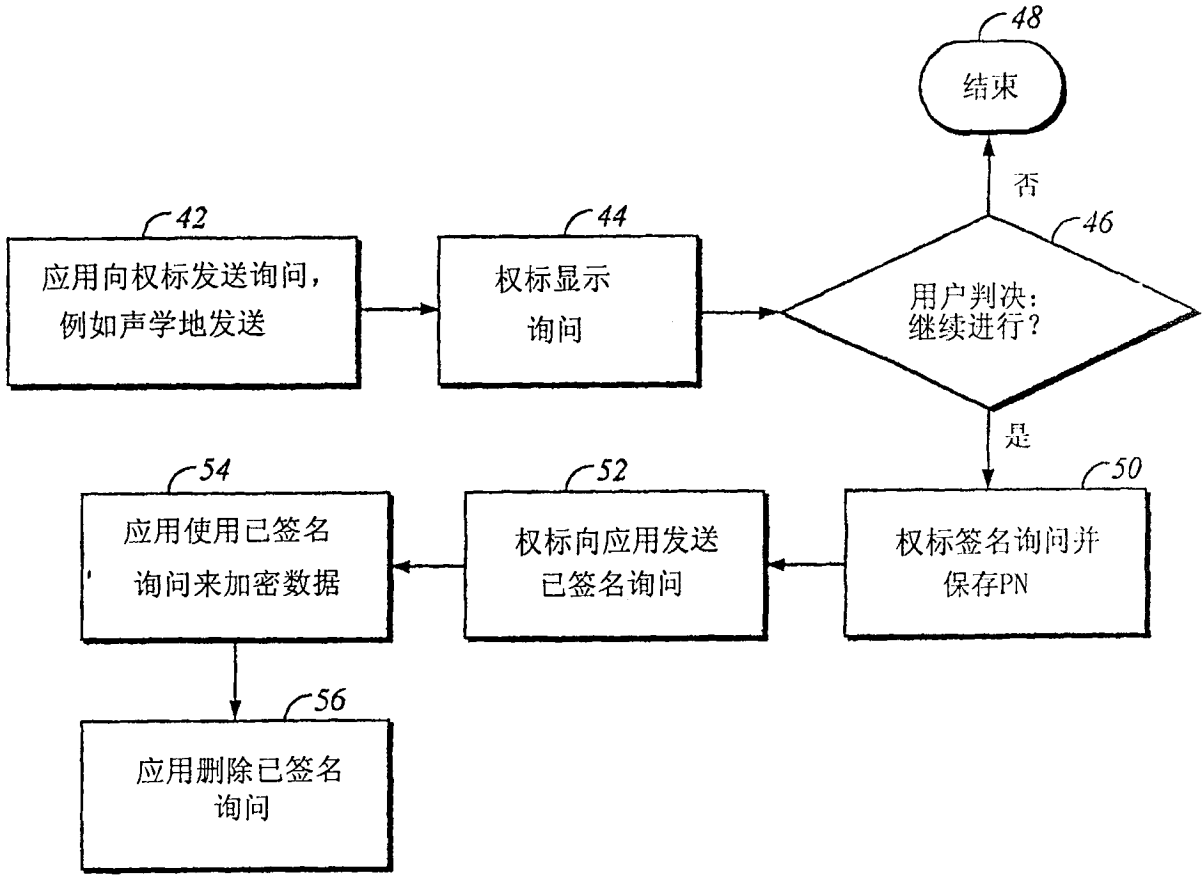

48
结束
否
46
用户判决：
继续进行？
是
42
应用向权标发送询问，
例如声学地发送
44
权标显示
询问
50
权标签名询问并
保存PN
52
权标向应用发送
已签名询问
54
应用使用已签名
询问来加密数据
56
应用删除已签名
询问

图 2

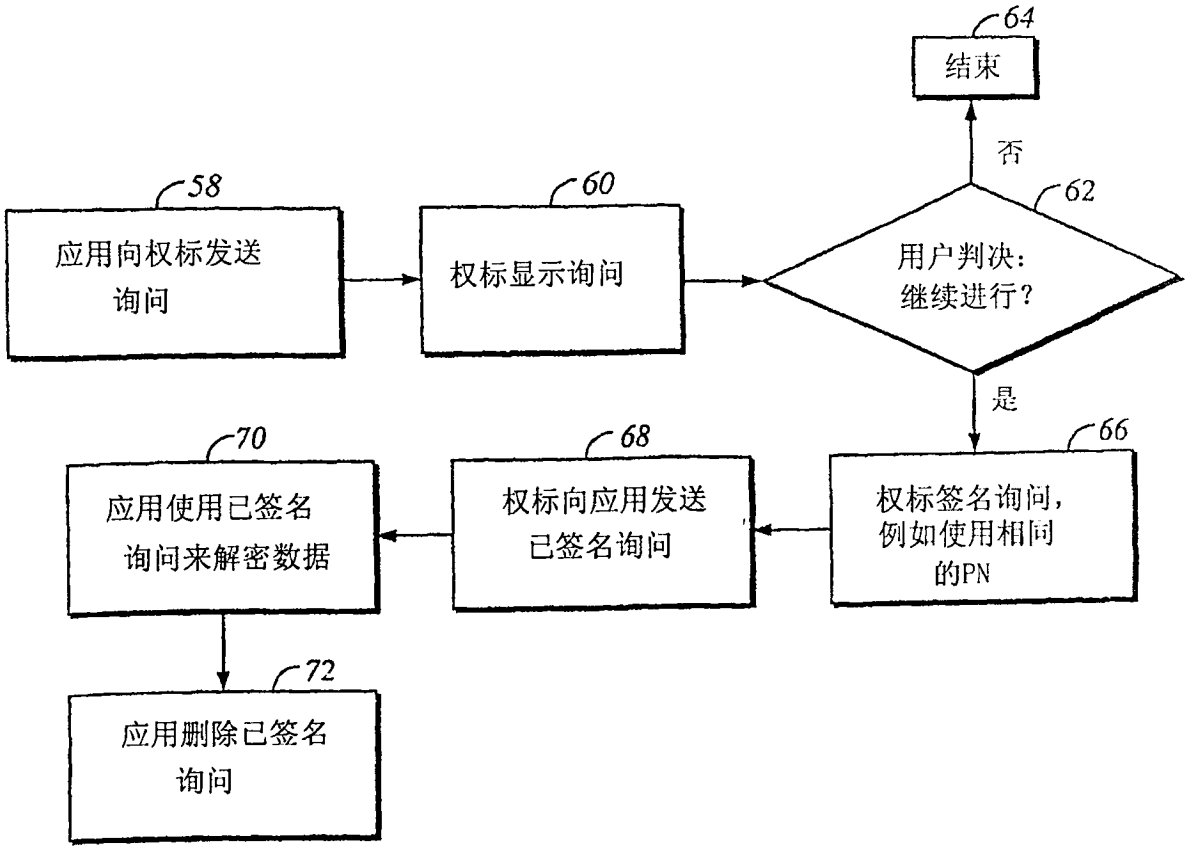

64
结束
否
62
58
60
应用向权标发送询问
权标显示询问
用户判决：继续进行？
是
66
70
68
应用使用已签名询问来解密数据
权标向应用发送已签名询问
权标签名询问，例如使用相同的PN
72
应用删除已签名询问

图 3