(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 101061663 B
(45)授权公告日 2011.11.02

(21)申请号 200480021026.9
(22)申请日 2004.07.21
(30)优先权数据
10/625,710 2003.07.22 US
10/785,313 2004.02.23 US
(85)PCT申请进入国家阶段日
2006.01.20
(86)PCT申请的申请数据
PCT/US2004/023580 2004.07.21
(87)PCT申请的公布数据
WO2005/013180 EN 2005.02.10
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 杰克·斯滕斯特罗
亚历山大·甘特曼
约翰·W·内伦贝格二世
艾哈迈德·贾拉利
格雷戈里·G·罗斯
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王英
(51)Int.Cl.
H04L 9/32(2006.01)
(56)对比文件
CN 1338841 A,2002.03.06, 全文.
US 5481611 A, 全文.
CN 1265762 A,2000.09.06, 全文.
US 5623637 A,1997.04.22, 全文.
审查员 宁波

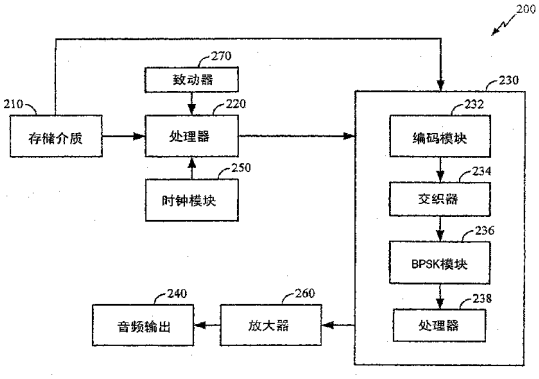
权利要求书 4 页 说明书 11 页 附图 12 页

(54)发明名称

通过声音信道进行数字认证

(57)摘要

公开了用于数字认证和验证的装置和方法。在一个实施例中,认证包括:存储加密密钥和查找表(LUT);使用所述加密密钥来生成访问码;基于所述访问码,生成多个并行的BPSK符号;使用所述LUT,将所述BPSK符号转换成用所述访问码编码的多个音调;输出用所述访问码编码的多个音调,以进行认证。在另一实施例中,验证包括:接收用访问码编码的多个音调;根据所述多个音调,生成多个并行的BPSK符号;将所述BPSK符号转换成所述访问码的编码交织比特流;将所述编码交织比特流进行解交织;从编码解交织比特流中恢复出所述访问码。



CN 101061663 B

1. 用于认证的装置，包括：

存储介质，用于存储加密密钥和查找表；

与所述存储介质相连的第一处理器，用于使用所述加密密钥来生成访问码；

与所述第一处理器相连的转换器，用于将所述访问码转换成用所述访问码编码的多个音调；以及

音频输出单元，用于输出用所述访问码编码的多个音调，以进行认证；

其中，所述转换器包括：

二进制移相键控模块，用于基于所述访问码生成多个并行的二进制移相键控符号；以及

与所述二进制移相键控模块和所述存储介质相连的第二处理器，用于使用所述查找表将所述二进制移相键控符号转换成所述多个音调。

2. 如权利要求 1 所述的装置，其中，所述第一或第二处理器中之一还将所述二进制移相键控符号重复选定次数；以及

其中，所述第二处理器将重复的二进制移相键控符号转换成所述多个音调。

3. 如权利要求 1 所述的装置，还包括：

与所述第一处理器相连的时钟模块，用于生成时间元素；以及

其中，所述第一处理器使用所述加密密钥和时间元素来生成所述访问码。

4. 如权利要求 3 所述的装置，还包括：

与所述第一处理器相连的致动器，用于接收用户命令；以及

其中，当收到所述用户命令时，所述第一处理器生成所述访问码。

5. 如权利要求 1 所述的装置，还包括：

容纳部件，用于包含所述存储介质、所述第一处理器、所述转换器和所述音频输出单元；以及

穿过所述容纳部件的孔。

6. 如权利要求 4 所述的装置，还包括：

与所述第一处理器相连的显示模块，用于显示所述访问码。

7. 如前述任一权利要求所述的装置，还包括：

用户输入端，用于接收个人标识号；

其中，所述转换器将所述个人标识号转换成用所述个人标识号编码的多个音调；以及

其中，所述音频输出单元还输出用所述个人标识号编码的多个音调，以进行认证。

8. 用于认证的装置，包括：

存储介质，用于存储加密密钥和查找表；

与所述存储介质相连的处理器，用于使用所述加密密钥来生成访问码；

与所述处理器相连的转换器，其中，所述转换器包括二进制移相键控模块，用于基于所述访问码生成多个并行的二进制移相键控符号，并且其中，所述处理器用于使用所述查找表将所述二进制移相键控符号转换成用所述访问码编码的多个音调；以及

音频输出单元，用于输出用所述访问码编码的多个音调，以进行认证。

9. 用于认证的方法，包括：

存储加密密钥和查找表；

使用所述加密密钥来生成访问码；

基于所述访问码，生成多个并行的二进制移相键控符号；

使用所述查找表，将所述二进制移相键控符号转换成用所述访问码编码的多个音调；以及

输出用所述访问码编码的多个音调，以进行认证。

10. 如权利要求 9 所述的方法，包括：

在转换所述二进制移相键控符号之前，将所述二进制移相键控符号重复选定次数。

11. 如权利要求 10 所述的方法，其中，重复所述二进制移相键控符号的步骤包括：将一组三二进制移相键控符号重复所述选定次数；以及

其中，转换所述二进制移相键控符号的步骤包括：使用所述查找表，将每组三二进制移相键控符号转换成所述多个音调。

12. 如权利要求 9 所述的方法，还包括：

将具有参考相位的参考音调加上所述多个音调；以及

将所述参考音调与所述多个音调一起输出。

13. 如权利要求 9 所述的方法，还包括生成时间元素；以及

其中，生成所述访问码的步骤包括：使用所述加密密钥和时间元素来生成所述访问码。

14. 如权利要求 13 所述的方法，还包括接收用户命令；以及

其中，生成所述访问码的步骤包括：当收到所述用户命令时，生成所述访问码。

15. 如权利要求 9 或其从属权利要求 10-14 中任意一项所述的方法，还包括：

接收个人标识号；

将所述个人标识号转换成用所述个人标识号编码的多个音调；以及

输出用所述个人标识号编码的多个音调，以进行认证。

16. 用于认证的装置，包括：

存储介质，用于存储加密密钥；

与所述存储介质相连的处理器，用于使用所述加密密钥来生成访问码；

与所述处理器相连的转换器，用于将所述访问码转换成用所述访问码编码的多个音调；以及

与所述转换器相连的音频输出单元，用于输出用所述访问码编码的多个音调，以进行认证；

其中，所述转换器包括：

二进制移相键控模块，用于基于所述访问码生成多个并行的重复二进制移相键控符号；

与所述二进制移相键控模块相连的快速傅立叶反变换模块，用于对重复的二进制移相键控符号执行快速傅立叶反变换，以生成代码符号；以及

与所述快速傅立叶反变换模块相连的上变频器，用于将所述代码符号调制成用所述访问码编码的多个音调。

17. 用于认证的方法，包括：

存储加密密钥；

使用所述加密密钥来生成访问码；

基于所述访问码，生成多个并行的二进制移相键控符号；

将所述二进制移相键控符号重复选定次数；

对重复的二进制移相键控符号执行快速傅立叶反变换，以生成快速傅立叶反变换符号；

将所述快速傅立叶反变换符号调制成用所述访问码编码的多个音调；以及

输出用所述访问码编码的多个音调，以进行认证。

18. 用于验证的装置，包括：

音频输入单元，用于接收用访问码编码的多个音调；

与所述音频输入单元相连的转换器，用于从用所述访问码编码的多个音调中恢复出所述访问码；以及

其中，所述转换器包括：

下变频器，用于将所述多个音调解调成快速傅立叶反变换符号；

快速傅立叶变换模块，用于根据所述快速傅立叶反变换符号生成多个并行的二进制移相键控符号；

与所述快速傅立叶变换模块相连的二进制移相键控模块，用于将所述二进制移相键控符号转换成所述访问码的编码交织比特流；

与所述二进制移相键控模块相连的解交织器，用于将所述编码交织比特流进行解交织；以及

与所述解交织器相连的解码模块，用于从编码解交织比特流中恢复出所述访问码。

19. 如权利要求 18 所述的装置，还包括：

存储介质，用于存储加密密钥；

与所述存储介质和所述转换器相连的处理器，用于使用所述加密密钥来验证所述访问码，并且，如果证实了所述访问码，则准予访问。

20. 如权利要求 19 所述的装置，其中，所述音频输入单元还接收用个人标识号编码的多个音调；

其中，所述转换器还从用所述个人标识号编码的多个音调中恢复出所述个人标识号；以及

其中，如果证实了所述访问码和所述个人标识号，则所述处理器也准予访问。

21. 如权利要求 20 所述的装置，还包括：

与所述处理器相连的时钟模块，用于生成时间元素；以及

其中，所述处理器使用所述加密密钥和时间元素来验证所述访问码。

22. 如权利要求 18 或其从属权利要求 19-21 中任意一项所述的装置，其中，所述快速傅立叶变换模块将所述快速傅立叶反变换符号转换成多组重复二进制移相键控符号，并生成一组选定二进制移相键控符号；以及

其中，所述二进制移相键控模块转换该组选定二进制移相键控符号。

23. 一种用于验证的方法，包括：

接收用访问码编码的多个音调；

通过对所述多个音调执行快速傅立叶变换来根据所述多个音调，生成多个并行的二进制移相键控符号；

将所述二进制移相键控符号转换成所述访问码的编码交织比特流；

将所述编码交织比特流进行解交织；以及

从编码解交织比特流中恢复出所述访问码。

24. 如权利要求 23 所述的方法，其中，执行快速傅立叶变换的步骤包括：生成重复的二进制移相键控符号；

其中，所述方法还包括：根据重复的二进制移相键控符号，生成一组选定二进制移相键控符号；以及

其中，转换所述二进制移相键控符号的步骤包括：将该组选定二进制移相键控符号转换成编码交织比特流。

25. 如权利要求 24 所述的方法，其中，执行快速傅立叶变换的步骤包括：

根据所述接收的多个音调生成快速傅立叶反变换符号；以及

将所述快速傅立叶反变换符号转换成多组重复的三二进制移相键控符号，其中，生成该组选定二进制移相键控符号的步骤包括：从这些组重复的三二进制移相键控符号中选择三个二进制移相键控符号，以生成该组选定二进制移相键控符号。

26. 如权利要求 24 所述的方法，其中，执行快速傅立叶变换的步骤包括：

根据所述接收的多个音调生成快速傅立叶反变换符号；以及

将所述快速傅立叶反变换符号转换成多组重复的三二进制移相键控符号，其中，生成该组选定二进制移相键控符号的步骤包括：选择所述多组重复的三二进制移相键控符号中的一组重复的三二进制移相键控符号，以生成该组选定二进制移相键控符号。

27. 如权利要求 23 所述的方法，还包括：

存储加密密钥；

用所述加密密钥来验证所述访问码；以及

如果证实了所述访问码，则准予访问。

28. 如权利要求 23 或其从属权利要求 24-27 中任意一项所述的方法，还包括：

接收用个人标识号编码的多个音调；

从用所述个人标识号编码的多个音调中恢复出所述个人标识号；以及

如果证实了所述访问码和所述个人标识号，则准予访问。

29. 如权利要求 27 所述的方法，还包括：

生成时间元素；以及

其中，验证所述访问码的步骤包括：使用所述加密密钥和时间元素来验证所述访问码。

通过声音信道进行数字认证

发明领域

[0001] 本发明一般涉及认证，尤其涉及使用声音对实体进行数字认证。

技术背景

[0002] 随着电子商务的增长，使用诸如互联网之类的公共通信基础设施来访问各种安全网络、系统和/或应用也在增长。例如，通过数字认证，用户可以经由公共通信网络（在线地或通过自动柜员机 ATM）访问银行、诸如内部网之类的私有网络、安全服务器或数据库、和/或其他虚拟专用网（VPN）。

[0003] 但是，由于采用了无法进行面对面接触的通信系统，所以，欺诈或非法访问的机会也增加了。如果被盗用的身份落入不法分子之手，则会对个人、组织或其他实体造成损害。

[0004] 为了防止不法访问，过去开发了各种验证用户或实体身份的安全机制，从而，只对授权实体准许访问。诸如令牌之类的访问码生成设备可以实现一种用户认证和访问控制技术。在这里，定期地生成唯一的访问码，并将其显示给用户。通常，访问码是根据基于安全信息和当前时间的算法而生成的。然后，用户需要输入当前显示的访问码才能进行访问。

[0005] 在有些系统中，进行访问还需要密码。这种类型的系统被称为双因素认证（two-factor authentication）。双因素认证通常基于：例如，用户有令牌；例如，用户知道密码。由于这两条信息都用于认证用户，所以，与单因素认证相比，执行双因素认证的系统不易受到攻击。

[0006] 上面描述的令牌可以防止未授权访问，但却很麻烦，因为用户在每次访问期间必须手工输入每个访问码。此外，由于手工输入访问码，所以更容易出现错误。在有些系统中，用户在每次访问期间需要不止一次地输入访问码，这增加了不便和出错概率。此外，由于访问码可以基于时间且连续显示，所以，令牌可能需要不断的计算，从而降低了令牌的电池寿命。

[0007] 因此，需要更高效、更便利和/或更安全的方式来使用设备实现控制访问系统。

发明内容

[0008] 这里公开的实施例通过提供数据处理系统中的安全方法，从而解决上述需求。

[0009] 在一个方面中，一种用于认证的装置，包括：存储介质，用于存储加密密钥和查找表（LUT）；与所述存储介质相连的第一处理器，用于使用所述加密密钥来生成访问码；与所述处理器相连的转换器，用于将所述访问码转换成用所述访问码编码的多个音调；音频输出单元，用于输出用所述访问码编码的多个音调，以进行认证；其中，所述转换器可以包括：二进制移相键控（BPSK）模块，用于生成多个并行的 BPSK 符号；与所述 BPSK 模块和所述存储介质相连的第二处理器，用于使用所述 LUT 将所述 BPSK 符号转换成多个音调。在这里，所述第一或第二处理器中之一可以将所述 BPSK 符号重复选定次数；然后，所述第二处理器将重复的 BPSK 符号转换成所述多个音调。

[0010] 在另一实施例中，一种用于认证的装置可以包括：存储介质，用于存储加密密钥和

查找表 (LUT) ;与所述存储介质相连的处理器,用于使用所述加密密钥来生成访问码 ;与所述处理器相连的转换器,用于将所述访问码转换成用所述访问码编码的多个音调 ;音频输出单元,用于输出用所述访问码编码的多个音调,以进行认证 ;其中,所述转换器包括 :二进制移相键控 (BPSK) 模块,用于生成多个并行的 BPSK 符号 ;其中,所述处理器使用所述 LUT 将所述 BPSK 符号转换成多个音调。

[0011] 在另一实施例中,一种用于认证的方法可以包括 :存储加密密钥和查找表 (LUT) ;使用所述加密密钥来生成访问码 ;基于所述访问码,生成多个并行的 BPSK 符号 ;使用所述 LUT,将所述 BPSK 符号转换成用所述访问码编码的多个音调 ;输出用所述访问码编码的多个音调,以进行认证。该方法还可以包括 :在转换所述 BPSK 符号之前,将所述 BPSK 符号重复选定次数。在这里,重复所述 BPSK 符号的步骤可以包括 :将一组三 BPSK 符号重复选定次数 ;其中,转换所述 BPSK 符号的步骤可以包括 :使用所述 LUT,将每组三 BPSK 符号转换成多个音调。

[0012] 在另一实施例中,一种用于认证的装置可以包括 :用于存储加密密钥和查找表 (LUT) 的模块 ;用于使用所述加密密钥来生成访问码的模块 ;用于基于所述访问码生成多个并行 BPSK 符号的模块 ;用于使用所述 LUT 将所述 BPSK 符号转换成用所述访问码编码的多个音调的模块 ;输出模块,用于输出用所述访问码编码的多个音调,以进行认证。该装置还可以包括用于将所述 BPSK 符号重复选定次数的模块,其中,用于转换所述 BPSK 符号的模块转换重复的 BPSK 符号。

[0013] 在另一实施例中,一种用于认证的装置可以包括 :存储介质,用于存储加密密钥 ;与所述存储介质相连的处理器,用于使用所述加密密钥来生成访问码 ;与所述处理器相连的转换器,用于将所述访问码转换成用所述访问码编码的多个音调 ;与所述转换器相连的音频输出单元,用于输出用所述访问码编码的多个音调,以进行认证 ;其中,所述转换器可以包括 :二进制移相键控 (BPSK) 模块,用于基于所述访问码生成多个并行的重复 BPSK 符号 ;与所述 BPSK 模块相连的快速傅立叶反变换 (IFFT) 模块,用于对重复的 BPSK 符号执行 IFFT,以生成代码符号 ;与所述 IFFT 模块相连的上变频器,用于将所述代码符号调制成用所述访问码编码的多个音调。

[0014] 在另一实施例中,一种用于认证的方法可以包括 :存储加密密钥 ;使用所述加密密钥来生成访问码 ;基于所述访问码,生成多个并行的二进制移相键控 (BPSK) 符号 ;在转换所述 BPSK 符号之前,将所述 BPSK 符号重复选定次数 ;对重复的 BPSK 符号执行快速傅立叶反变换 (IFFT),以生成 IFFT 符号 ;将所述 IFFT 符号调制成用所述访问码编码的多个音调 ;输出用所述访问码编码的多个音调,以进行认证。

[0015] 在另一实施例中,一种用于认证的装置可以包括 :用于存储加密密钥的模块 ;用于使用所述加密密钥来生成访问码的模块 ;用于基于所述访问码生成多个并行二进制移相键控 (BPSK) 符号的模块 ;用于在转换所述 BPSK 符号之前将所述 BPSK 符号重复选定次数的模块 ;用于对重复的 BPSK 符号执行快速傅立叶反变换 (IFFT) 以生成 IFFT 符号的模块 ;用于将所述 IFFT 符号调制成用所述访问码编码的多个音调的模块 ;用于输出用所述访问码编码的多个音调以进行认证的模块。

[0016] 在另一实施例中,一种用于验证的装置可以包括 :音频输入单元,用于接收用访问码编码的多个音调 ;与所述音频输入单元相连的转换器,用于从用访问码编码的多个音调

中恢复出所述访问码；其中，所述转换器包括：下变频器，用于将所述多个音调解调成 IFFT 符号；快速傅立叶变换（FFT）模块，用于根据所述 IFFT 符号生成多个并行的 BPSK 符号；与所述处理器相连的 BPSK 模块，用于将所述 BPSK 符号转换成所述访问码的编码交织比特流；与所述 BPSk 模块相连的解交织器，用于将所述编码交织比特流进行解交织；与所述解交织器相连的解码模块，用于从所述编码解交织比特流中恢复出所述访问码。该装置还可以包括：存储介质，用于存储加密密钥；与所述存储介质和所述转换器相连的处理器，用于使用所述加密密钥来验证所述访问码，并且，如果证实了所述访问码，则准予访问。此外，所述 FFT 模块将所述多个音调转换成多组重复 BPSK 符号，并生成一组选定 BPSK 符号；其中，所述 BPSK 模块转换该组选定 BPSK 符号。

[0017] 在另一实施例中，一种用于验证的方法可以包括：接收用访问码编码的多个音调；根据所述多个音调，生成多个并行的 BPSK 符号；将所述 BPSK 符号转换成所述访问码的编码交织比特流；将所述编码交织比特流进行解交织；从所述编码解交织比特流中恢复出所述访问码。在这里，执行 FFT 的步骤包括：生成重复的 BPSK 符号；其中，所述方法还包括：根据重复的 BPSK 符号，生成一组选定 BPSK 符号；其中，执行所述 BPSK 的步骤包括：将该组选定 BPSK 符号转换成编码交织比特流。此外，执行 FFT 的步骤包括：将所述 IFFT 符号转换成多组重复的三 BPSK 符号；其中，生成该组选定 BPSK 符号的步骤包括：从这些组重复的三 BPSK 符号中选择三个 BPSK 符号，以生成该组选定 BPSK 符号。或者，执行所述 FFT 的步骤包括：将所述 IFFT 符号转换成多组重复的三 BPSK 符号；其中，生成该组选定 BPSK 符号的步骤包括：选择一组重复的三 BPSK 符号，以生成该组选定 BPSK 符号。

[0018] 在另一实施例中，一种用于验证的装置可以包括：用于接收用访问码编码的多个音调的模块；用于根据所述多个音调生成多个并行 BPSK 符号的模块；用于将所述 BPSK 符号转换成所述访问码的编码交织比特流的模块；用于将所述编码交织比特流进行解交织的模块；用于从所述编码解交织比特流中恢复出所述访问码的模块。

[0019] 附图简述

[0020] 下面将结合附图详细描述各个实施例，在这些附图中，相同的标记指的是相同的部件，其中：

[0021] 图 1 示出了通过声音信道进行数字认证的系统；

[0022] 图 2 示出了令牌的一个示例性实施例；

[0023] 图 3 示出了验证机的一个示例性实施例；

[0024] 图 4 示出了使用声音信道进行数字认证的示例性方法；

[0025] 图 5A 和 5B 示出了 BPSK 符号的示例；

[0026] 图 5C 示出了 LUT 的示例；

[0027] 图 6 示出了使用声音信道进行数字验证的示例性方法；

[0028] 图 7A 和 7B 示出了原始的重复 BPSK 符号组和已恢复的重复 BPSK 符号组；

[0029] 图 7C 和 7D 示出了选定 BPSK 符号组的示例；

[0030] 图 8 示出了令牌的一个示例性实施例；

[0031] 图 9 示出了使用声音信道进行数字认证的另一示例性方法；

[0032] 图 10 示出了使用声音信道进行数字验证的一个示例性方法；

[0033] 图 11A 至 11D 示出了通过声音信道进行数字认证的其他示例性系统；

[0034] 图 12 示出了接收机的一个示例性实施例；

[0035] 图 13 示出了接收机的另一实施例；以及

[0036] 图 14A 和 14B 示出了令牌的示例性外壳。

具体实施方式

[0037] 通常情况下，所公开的实施例使用声音信道，对用户或实体进行数字认证。在下面的说明中，给出了具体的细节，以便于透彻理解这些实施例。但是，本领域技术人员应当理解的是，这些实施例也可以不用这些具体细节来实现。例如，可以用框图形式给出电路，从而不使不必要的细节模糊这些实施例。但在其他实例中，为了更好地解释这些实施例，可以详细地给出公知的电路、结构和技术。

[0038] 还应当注意的是，可以将这些实施例描述成用流程图、结构图或框图表示的过程。尽管流程图可以将多个操作描述为顺序的过程，但其中的很多操作可以并行或同时执行。此外，可以重新排定操作的次序。当操作完成时，过程结束。过程可以对应于方法、函数、程序、子例程、子程序等。当过程对应于函数时，其结束对应于该函数返回主调函数或主函数。

[0039] 此外，就如同这里所披露的那样，术语“声波”指的是通过气体、液体或固体行进的声学波或压力波或振动。声波包括超声波、音频波和亚声波。术语“音频波”指的是处于声谱之内的声波频率，大约是 20Hz 至 20kHz。术语“超声波”指的是高于声谱的声波频率。术语“亚声波”指的是低于声谱的声波频率。术语“存储介质”表示一种或多种用于存储数据的器件，包括用于存储信息的只读存储器 (ROM)、随机访问存储器 (RAM)、磁盘存储介质、光存储介质、闪存和 / 或其他机器可读介质。术语“机器可读介质”包括、但不限于便携式或固定的存储器件、光存储器件、无线信道和各种其他器件，它们能够存储、容纳或承载指令和 / 或数据。术语“音调”指的是具有特定调子和振动的声波载波信号，其承载数字数据。术语“多个音调”指的是三个或更多音调。术语“认证”指的是实体的认证，术语“认证”和“验证”可以互换地使用。

[0040] 图 1 示出了通过声音信道进行数字认证的示例性系统 100。在系统 100 中，验证机设备 110 控制通过诸如互联网 120 之类的公共通信基础设施访问安全网络、系统和 / 或应用。尽管可以通过除互联网 120 之外的公共通信设施进行访问，但出于说明目的，将参考互联网 120 来描述系统 100。

[0041] 为了通过互联网 120 进行访问，诸如令牌 130 之类的设备通过无线通信设备 (WCD) 140 向验证机设备 110 提供访问码。访问码通过声音信道从令牌 130 传送到 WCD 140。使用令牌 130 中安全存储的加密密钥来生成访问码，并将其编码成声波，以进行通信。更具体地说，使用多载波调制将生成的访问码编码成多个音调，使用对应的多载波解调从所述多个音调中恢复出访问码。

[0042] 令牌 130 的用户还可以向验证机设备 110 提供用户信息，如用户名。在这里，可以将用户信息编码成声波，并将其与访问码一起传送到 WCD 140。或者，也可以将用户信息直接输入 WCD 140 中。然后，WCD 140 可以通过互联网 120 将访问码和用户信息转发给验证机 110，以进行认证。在其他实施例中，用户信息可以是令牌 130 的分配标识号。因此，用户不必输入用户信息。自动将标识号编码成声波，与访问码一起传送到 WCD 140。准予访问之后，WCD 140 可用于与安全网络或系统进行通信。

[0043] 为了转发访问码和/或用户信息，WCD 140可以从声波中恢复出访问码和/或用户信息，如果是经过编码的话。然后，WCD 140可以将访问码和/或用户信息转发给验证机设备110。或者，用访问码编码的声波和用用户信息编码的声波，如果是经过编码的话，可以传输到验证机设备110。于是，验证机设备110可以从声波中恢复出访问码和/或用户信息。在这里，访问码和/或用户信息，或用访问码和/或用户信息编码的声波，可以通过允许对系统100中的互联网120进行访问的任何公知通信技术来传输。

[0044] 令牌130通常是便携式设备，可能小得足以携带在口袋中和/或附加于钥匙链上。对令牌130的物理拥有提供了所需验证的一个方面，就如同对钥匙的物理拥有使得个人能够通过锁住的门来实现访问。因此，令牌130用作认证工具，并且，除了通过声波进行通信之外，令牌130不需要具有传统的无线通信能力，以通过互联网120或其他无线和有线基础设施直接向验证机设备110发送访问码。也就是说，在有些实施例中，令牌130不支持无线通信能力，并且不包括无线调制解调器、网卡和/或其他无线链路，通向私有或公用通信基础设施，如互联网120。所以，WCD 140通过互联网120发送访问码。但是，应当注意的是，在其他实施例中，令牌130也可以嵌入其他设备中，如无线电话或个人数字助理。此外，尽管所示的WCD 140是个人台式计算机，但它可以是各种其他计算机设备，例如、但不限于：膝上计算机、PDA、家庭、办公室或车辆无线电话或安全设备。

[0045] 访问码是用加密密钥生成的，加密密钥安全地存储在令牌130中。可以在制造时将加密密钥置入令牌130中，这是用户不知道的。这里，两种加密密钥可用于数字认证：对称密码系统和非对称密码系统。在对称密码系统中，在令牌130中处于保密状态的密钥或对称密钥，是共享的，并被放置到验证机设备110中。令牌130使用密钥来生成数字签名，并将数字签名发送给验证机设备110，以进行认证。验证机设备110基于相同的密钥，验证数字签名。在非对称密码系统中，为用户生成一个私钥和一个公钥。公钥是与验证机设备110共享的，而私钥在令牌130中处于保密状态。用私钥生成数字签名，并将其发送给验证机设备110。然后，验证机设备110基于用户的公钥，验证该数字签名。

[0046] 在上面的描述中，验证机设备110基于与访问码一起发送的用户信息，验证与用户相对应的加密密钥。也可以将验证机设备110实现成用户要访问的安全网络或系统的一部分。或者，验证机设备110可以位于安全网络或系统的外面。此外，尽管图1示出了一个验证机设备110，但是，对于本领域技术人员来说显而易见的是，可以有一个以上的验证机设备，每个设备控制对一个或多个网络/系统的访问。

[0047] 图2的框图示出了令牌300的一个示例性实施例，图3示出了验证机300的一个示例性实施例。令牌200可以包括：存储介质210，用于存储加密密钥和查找表(LUT)；处理器220，用于使用加密密钥来生成访问码；转换器230，用于使用LUT，将访问码转换成用访问码编码的多个音调；音频输出单元240，用于输出用访问码编码的多个音调，以进行验证。验证机设备300可以包括：存储介质310，用于存储加密密钥；处理器320，用于使用加密密钥来生成访问码；音频输入单元330，用于从令牌接收用访问码编码的多个音调；转换器340，用于从多个音调中恢复出访问码。基于加密密钥，处理器320检验用户的访问码。

[0048] 更具体地讲，基于多载波调制，将访问码转换成多个音调以及从多个音调进行转换。因此，转换器230将访问码调制成多载波信号，转换器340使用多载波系统，从多载波信号中解调出访问码。共同待决的美国申请No.10/356,144和共同待决的美国申请

No.10/356,425 中描述了一种多载波系统。在多载波调制中，待传输的数据流被分为多个交织比特流。这样，就得到了具有很低比特率的多个并行比特流。然后，将每个比特流用于调制多个载波，并通过不同的载波信号传输。通常，载波调制涉及对待传输的数据流进行编码、交织、数字调制、傅立叶反变换（IFFT）处理和上变频。解调涉及对收到的数据流进行下变频、FFT 处理、数字解调、解交织和解码。但是，在转换器 230 和 340 中，使用 LUT 来促进调制，如下所述。

[0049] 令牌 200 的转换器 230 可以包括编码模块 232、交织器 234、二进制移相键控（BPSK）模块 236 和处理器 238。验证机设备 300 的转换器 340 可以包括下变频器 341、FFT 模块 343、BPSK 模块 345、解交织器 347 和解码模块 349。BPSK 是一种易于实现的公知数字调制技术。尽管 BPSK 不会导致可用带宽的最高效利用，但却不易受噪声影响。因此，使用 BPSK 将代码符号转换成音调。但是，在转换器 230 和 340 中，也可以实现除 BPSK 之外的调制技术。此外，应当注意的是，转换器 230 示出了基于 BPSK 的简化多载波调制器。更典型的商用多载波调制器可以具有附加的部件，如前导码生成器、串并（S/P）转换器或并串（P/S）转换器。同样，转换器 340 示出了与转换器 230 相对应的简化多载波解调器，更典型的商用多载波解调器还可以具有附加的部件，如同步单元、S/P 转换器和 P/S 转换器。

[0050] 通常，编码模块 232 用于对比特流或访问码的比特流进行编码。然后，交织器 234 将编码的比特流交织成交织比特流或代码符号。BPSK 模块 236 根据代码符号，生成多个并行的 BPSK 符号。更具体地讲，将编码的比特流串并转换成并行的代码符号。然后，BPSK 模块 236 把并行的代码符号映射成多个并行的 BPSK 符号。这里，可以将代码符号映射成 BPSK 符号，然后串并转换成 BPSK 符号，或者，可以将代码符号进行串并转换，然后映射成为 BPSK 符号。此外，BPSK 符号的数量对应于多载波系统中可用音调的数量。在有些实施例中，多载波音调的频率范围大约为 1kHz 至 3kHz，每个载波允许的带宽取决于音调的数量。例如，如果可用音调数量是 64，则每个载波可以允许大约 31.25Hz 的带宽。由处理器 238 使用 LUT，将上述生成的多个 BPSK 符号转换成多个音调，并对其进行串并转换。通过实现 LUT，可以直接将 BPSK 符号转换成多个音调，而无需 IFFT 处理和上变频。下面将结合图 5 描述 LUT 的详细操作。

[0051] 为了恢复出访问码，转换器 340 执行的过程与转换器 230 执行的过程相反。即，下变频器 341 将多个音调解调成多个并行的 IFFT 符号；FFT 模块 343 执行 FFT，从而生成多个并行的 BPSK 符号；BPSK 模块 345 将 BPSK 符号转换成代码符号或访问码的编码交织比特流；解交织器 347 对代码符号进行解交织；解码模块 349 从编码的代码符号中恢复出访问码。更具体地说，下变频器 341 可以将多个音调解调为多个 IFFT 符号；S/P 对 IFFT 符号进行串并转换；FFT 模块 343 可以执行 FFT，以生成多个并行的 BPSK 符号；BPSK 模块 345 可以将 BPSK 符号转换成多个并行的代码符号；解交织器 347 可以将代码符号解交织成编码比特流；P/S 可以对代码符号进行并串转换，然后由解码模块 349 进行解码。或者，可以将多个音调进行：串并转换；FFT 处理成多个并行 BPSK 符号；并串转换；BPSK 处理，以进行解交织。再或者，可以对多个音调进行：并串转换；FFT 处理成多个并行 BPSK 符号；BPSK 处理成多个并行的代码符号；并串转换；解交织。

[0052] 在转换器 230 和 340 中，更典型的令牌和验证机设备可以具有附加的部件。在有些实施例中，令牌 200 还可以包括：放大器 260，用于将来自转换器 230 的多个音调进行放大；

激励器或致动器 270，用于从用户接收信号，以激活认证过程。致动器 260 可以是、但不限于：开关、按钮开关、拨动开关或拨号或声音激励设备。令牌 200 还可以包括时钟模块 250，用于生成时间元素。在这些情形中，处理器 220 可以使用加密密钥和时间元素来生成访问码。同样，验证机设备 300 还可以包括时钟模块 350，用于生成时间元素。在这些情形中，处理器 320 可以使用加密密钥和时间元素来生成访问码。

[0053] 将令牌 200 和验证机设备 300 中的时钟模块 250 和 350 进行同步，以根据需要定期生成一个时间元素，例如，每分钟、每小时、每天或其他选定的增量。这种认证通常被称为基于认证的会话，因为访问码随每个时间段而改变。此外，存储介质 210 和 310 可以是加密密钥的数据库，对应于网络、系统或应用的不同用户。因此，将用户信息发送给验证机设备 300，如上所述，从而在认证过程中，在验证机 300 中使用合适的加密密钥。

[0054] 图 4 示出了一个示例性方法 400，用于使用声音信道来发送访问码。对于访问安全网络、系统或应用，处理器 220 使用加密密钥，生成访问码 (410)。此后，基于该访问码，生成多个并行的 BPSK 符号 (420)，然后，使用 LUT，将这些 BPSK 符号转换成多个用访问码编码的音调 (430)。更具体地说，将访问码的比特流编码成编码比特流。可以对编码比特流进行：串并转换；交织成多个并行的代码符号；BPSK 映射成多个并行 BPSK 符号；使用 LUT，转换成多个音调。或者，可以对编码比特流进行：交织；BPSK 映射；然后串并转换成多个并行的 BPSK 符号，以转换成多个音调。再或者，对编码比特流可以进行：交织，然后串并转换成多个并行的代码符号，以进行 BPSK 处理。在这里，可以将加密密钥和 LUT 存储在存储介质 210 中，处理器 238 可以使用存储介质 210 中存储的 LUT，将 BPSK 符号转换成多个音调。然后，输出用访问码编码的多个音调，以进行认证 (440)。

[0055] 更具体地讲，预先计算出 LUT，以将 BPSK 符号映射成指定音调。例如，可以映射每个特定的 BPSK 符号序列，后者对应于一个不同的可用音调。因此，不是对 BPSK 符号执行 IFFT 和调制 IFFT 符号，LUT 将 BPSK 符号直接转换成多个音调。

[0056] 在有些实施例中，为了增强访问码的恢复，在转换这些 BPSK 符号之前，先将这些 BPSK 符号重复选定次数。然后，可以预先计算出 LUT，以将多组 BPSK 符号映射成多个音调。图 5A 至 5C 示出了从重复 BPSK 符号转换为对应音调的示例。假设 BPSK 符号序列 {01110010} 如图 5A 所示，将一组二 BPSK 符号 {01，11，00，10} 重复两次，得到重复的 BPSK 符号 {0101，1111，0000，1010}，如图 5B 所示。在 LUT 中可以找到这些重复的 BPSK 符号，从而转换成对应的音调。图 5C 给出了一个示例性的 LUT，可用于将这些组重复两次的 BPSK 符号进行转换。在这里，LUT 条目 0000-1111 中的每一个对应于音调 T1 ～ T16 中的一个。基于该 LUT，这些重复的 BPSK 符号将对应于音调 {T6，T16，T1，T11}。

[0057] 应当注意的是，如果 BPSK 符号非重复的话，则图 5A 所示的 BPSK 符号将对应于音调 {T8，T3}。此外，如果重复的话，则可以将 BPSK 重复两次以上。此外，可将两个以上的 BPSK 符号分组成一组 BPSK 符号，多组 BPSK 符号可以重复选定次数，以转换成多个音调。根据一组中成组 BPSK 符号的数量以及该组的重复次数，还可以调整 LUT。例如，一组三 BPSK 符号可以重复三次。在这种情况下，LUT 可以具有 512 个条目，范围为 000000000-111111111。然后，可以使用 LUT，将这些组重复的三 BPSK 符号转换成音调。

[0058] 为了进一步增强访问码的恢复，具有参考相位的参考音调可加入所述多个音调。然后，将参考音调和多个音调一起输出。此外，可以将多个音调进行放大，然后再输出多个

音调。此外，如果实现时钟模块的话，那么，处理器 220 使用加密密钥和时间元素来生成访问码。然后，当用户通过致动器 270 输入命令时，从令牌 200 中可以生成、转换和输出访问码。

[0059] 图 6 示出了一个示例性方法 600，用于使用声音信道来验证访问码。为了进行验证，通过音频输入模块 330，接收用访问码编码的多个音调 (610)。下变频器 341 将多个音调下变频或解调为多个并行的 IFFT 符号 (620)。然后，FFT 模块 343 执行 FFT，以生成多个并行的 BPSK 符号 (630)。BPSK 模块 345 将 BPSK 符号转换成编码的比特流或代码符号 (640)，然后，由解交织器 347 进行解交织 (650)。更具体地讲，可以对多个音调进行 ：解调 ；串并转换成多个并行的 IFFT 符号 ；FFT 处理成多个并行的 BPSK 符号 ；BPSK 映射成多个并行的代码符号 ；解交织成编码的代码符号。或者，对多个音调可以进行 ：解调 ；串并转换 ；IFFT 处理 ；然后，并串转换成 BPSK 符号，以进行解交织。再或者，对多个音调可以进行 ：解调 ；串并转换 ；FFT 处理 ；BPSK 映射 ；然后并串转换成多个并行的 BPSK 符号，以进行解交织。此后，解码模块 349 从编码的代码符号中恢复出访问码 (660)。然后，处理器 320 使用加密密钥来验证访问码 (670)，如果证实了访问码，则准予访问 (680)。在这里，加密密钥可以存储在存储介质 310 中。

[0060] 在方法 600 中，如果重复 BPSK 符号以进行转换，则对多个音调进行解调和 FFT 处理，得到重复的 BPSK 符号。然后，根据重复的 BPSK 符号，生成一组选定的 BPSK 符号，并将该组选定的 BPSK 符号转换成代码符号或编码交织比特流。在这里，BPSK 模块 345 可以根据重复的 BPSK 符号，生成该组选定的 BPSK 符号，并将该选定组转换成代码符号。图 7A 至 7D 示出了如何生成该组选定的 BPSK 符号。

[0061] 如图所示，把一组两 BPSK 符号进行两次重复，得到原始的 BPSK 符号 A1B1A2B2C1D1C2D2，然后，将其解调为 A′ 1B′ 1A′ 2B′ 2C′ 1D′ 1C′ 2D′ 2。通过选择这两组重复 BPSK 符号中的一组，可以生成选定的 BPSK 符号，如图 7C 所示。或者，从任一组重复 BPSK 符号中选择每个 BPSK 符号，可以生成选定的 BPSK 符号，如图 7D 所示。在这里，应当注意的是，可以将多个音调转换成多组两个以上 BPSK 符号。例如，可以将多个音调转换成多组重复的三 BPSK 符号。在这种情况下，通过从这些组重复的三 BPSK 符号中选择每个 BPSK 符号，可以生成该组选定的 BPSK 符号。或者，通过选择一组重复的三符号，可以生成该组选定的 BPSK 符号。

[0062] 此外，如果收到具有参考相位的参考音调，则使用参考音调，将多个音调转换成多个 BPSK 符号。此外，如果实现了时钟模块，则处理器 320 使用加密密钥和时间元素来验证访问码。

[0063] 如果令牌的处理能力或速度有限，则 LUT 可以使用多个音调发送访问码来大大提高效率和性能。但是，有些实施例可能未实现和使用 LUT。图 8 示出了未使用 LUT 的令牌 800 的另一示例性实施例。

[0064] 令牌 800 包括 ：存储介质 810，用于存储加密密钥 ；处理器 820，用于使用加密密钥来生成访问码 ；转换器 830，用于将访问码转换成多个音调 ；音频输出单元 840，用于输出用访问码编码的多个音调，以进行验证。在有些实施例中，令牌 800 可以包括 ：放大器 860、激励器或致动器 870 以及时钟模块 880，就如同令牌 200 的放大器 260、致动器 270 和时钟模块 280 所实现的那样。

[0065] 通常，令牌 800 实现的部件与令牌 200 中的部件相同。但是，转换器 830 的调制没有基于 LUT。因此，不必将 LUT 存储在存储介质 810 中。此外，转换器 830 的处理基于使用重复的 BPSK 符号。更具体地讲，令牌 800 的转换器 830 可以包括：编码模块 83，用于对访问码的比特流进行编码；交织器 833，用于将编码比特流进行交织；BPSK 模块 835，用于将交织比特流或代码符号转换成 BPSK 符号，以及生成选定数量组的重复 BPSK 符号；IFFT 模块 837，用于对重复的 BPSK 符号执行 IFFT；上变频器 839，用于将 IFFT 符号调制成用访问码编码的多个音调。

[0066] 因此，对编码比特流进行串并转换，然后映射成多个并行的 BPSK 符号。根据各并行 BPSK 符号，生成选定数量组的重复 BPSK 符号。即，生成多组并行的重复 BPSK 符号，对应于多个并行的 BPSK 符号。然后，可以对多组重复的 BPSK 符号进行 IFFT 处理，以及并串转换，以供输出。在这里，可以将代码符号映射成 BPSK 符号，然后串并转换成 BPSK 符号，或者，可以对代码符号进行串并转换，然后映射成 BPSK 符号。

[0067] 图 9 示出了一个示例性方法 900，对应于令牌 800 通过声音信道发送访问码。对于访问安全网络、系统或应用，处理器 820 使用加密密钥，生成访问码 (910)。此后，基于该访问码，生成多组并行重复的 BPSK 符号 (920)，并执行 IFFT 变换，以生成 IFFT 符号 (930)。然后，将 IFFT 符号调制成多个用访问码编码的音调 (940)，音频输出单元 840 可以输出多个音调，以供认证 (980)。这里，加密密钥可以存储在存储介质 810 中。

[0068] 更具体地讲，对访问码的比特流可以进行编码、串并转换、交织和 BPSK 映射成多个并行的 BPSK 符号。每个并行的 BPSK 符号被重复选定次数，如图 5A 至 5C 所示，从而生成多组并行重复的 BPSK 符号，以进行 IFFT 处理。或者，可以对编码比特流进行交织、BPSK 映射，然后串并转换成多个并行 BPSK 符号，以进行重复。再或者，可以对编码比特流进行交织、然后串并转换成多个并行代码符号，以进行 BPSK 处理。

[0069] 此外，与令牌 200 中一样，可将具有参考相位的参考音调加入多个音调。然后，将参考音调和多个音调一起输出。此外，可以将多个音调放大，然后输出多个音调。此外，如果实现时钟模块的话，处理器 820 使用加密密钥和时间元素，生成访问码。然后，当用户通过致动器 870 输入命令时，从令牌 800 中可以生成、转换和输出访问码。

[0070] 虽然转换器 830 的调制不基于使用 LUT，但验证机设备 300 可以执行调制和相应的方法 600，如图 3 和 6 所示。因此，与转换器 830 相对应的转换器 340 可以包括：下变频器 341，用于将多个音调解调成 IFFT 符号；FFT 模块 343，用于执行 FFT，以生成重复的 BPSK 符号；BPSK 模块 345，用于根据重复的 BPSK 符号，生成一组选定的 BPSK 符号，并将该组选定的 BPSK 符号转换成代码符号或访问码的编码交织比特流；解交织器 347，用于将代码符号进行解交织；解码模块 349，用于从编码解交织比特流中恢复出访问码。与令牌 200 中一样，在转换器 830 和 340 中也可以实现除 BPSK 之外的调制技术。

[0071] 图 10 示出了示例性方法 1000，对应于转换器 830 使用声音信道验证访问码。为了进行验证，通过音频输入模块 330 接收用访问码编码的多个音调 (1010)。下变频器 341 将这多个音调下变频或解调成 IFFT 符号 (1020)。然后，FFT 模块 343 执行 FFT，以生成重复的 BPSK 符号 (1030)，此后，根据重复的 BPSK 符号，生成一组选定的 BPSK 符号 (1040)。在这里，可以生成该组选定的 BPSK 符号，如图 7A 至 7D 所示。BPSK 模块 345 将选定的 BPSK 符号转换成编码交织比特流或访问码的代码符号 (1050)。此后，解交织器 347 将编码交织比

特流进行解交织 (1060)，解码模块 949 从编码解交织比特流中恢复出访问码 (1070)。处理器 320 使用存储介质 910 中存储的加密密钥，验证访问码 (1080)，如果证实了访问码，则准予访问 (1090)。

[0072] 与验证机设备 300 中一样，如果收到具有参考相位的参考音调，则使用参考音调将多个音调转换成 IFFT 符号。然后，将参考音调和多个音调一起输出。此外，如果实现时钟模块的话，处理器 320 使用加密密钥和时间元素，验证访问码。

[0073] 如上所述，可以将访问码和 / 或密码 :编码成多个音调 ;通过诸如互联网 120 之类的公共通信设施传输 ;从多个音调中恢复出来 ;进行验证，以访问安全网络、系统和 / 或应用。

[0074] 系统 100 只是一个示例，还可以有其他通过声音信道进行数字认证系统。图 11A 至 11D 示出了通过声音信道的其他示例性数字认证系统。在图 11A 中，可以从令牌 1110 把用访问码编码的多个音调输出和发送到接收机设备 1120。然后，通过无线或有线通信基础设备 1140，将访问码从接收机设备 1120 转发到验证机设备 1130。在图 11B 中，从令牌 1110 输出用访问码编码的多个音调，并通过无线或有线电话 1150 将其传输给接收机 1120。此后，通过无线或有线通信基础设备 1140，从接收机设备 1120 将访问码转发到验证机设备 1130。在图 11A 和图 11B 中，接收机设备 1120 远离验证机设备 1130。在有些情况下，接收机设备 1120 可以远离验证机设备 1130，或者是验证机设备 1130 的一部分，如图 11C 所示。在图 11C 中，令牌 1110 将用访问码编码的多个音调直接输出到接收机 / 验证机设备 1160。或者，也可以通过无线或有线电话 1150，从令牌 1110 输出用访问码编码的多个音调，并传输到接收机 / 验证机 1160。

[0075] 因此，用访问码编码的多个音调可以从接收机设备 1120 转发到验证机设备 1130，验证机设备 1130 可以恢复出访问码。在有些实施例中，可以先从多个音调中恢复出访问码，然后，将恢复出来的访问码从接收机设备 1120 转发到验证机设备 1130，以进行认证。图 12 示出了与令牌 200 相对应的接收机 1200 的一个示例，图 13 示出了与令牌 800 相对应的接收机 1300 的一个示例，用于恢复访问码。

[0076] 接收机 1200 包括 :存储介质 1210，用于存储与存储介质 210 中的 LUT 相对应的 LUT ;音频输入单元 1220，用于从令牌用户接收用访问码编码的多个音调 ;转换器 1230，用于使用 LUT，从多个音调中恢复访问码。转换器 1230 可以包括 :处理器 1232，用于使用 LUT，将多个音调转换成 BPSK 符号 ;BPSK 模块，用于基于 BPSK，执行解调，从而将 BPSK 符号转换成代码符号或访问码的编码交织比特流 ;解交织器 1236，用于对代码符号进行解交织 ;解码模块 1238，用于从编码代码符号中恢复出访问码。

[0077] 接收机 1300 包括 :音频输入单元，用于从令牌用户接收用访问码编码的声波 ;转换器 1320。转换器 1320 可以包括 :下变频器 1321，用于将多个音调解调成 IFFT 符号 ;FFT 模块 1323，用于执行 FFT，以生成重复的 BPSK 符号 ;BPSK 模块 1325，用于根据重复的 BPSK 符号，生成一组选定的 BPSK 符号，并将该组的选定 BPSK 符号转换成访问码的编码交织比特流 ;解交织器 1327，用于将编码交织比特流进行解交织 ;解码模块 1329，用于从编码解交织比特流中恢复出访问码。

[0078] 通常，与用于恢复访问码的接收机 1200 相对应的方法也对应于图 6 所述的方法。但是，接收机 1200 不对恢复出来的访问码进行验证，并且不基于访问码授权访问。同样，

与用于恢复访问码的接收机 1300 相对应的方法也对应于图 11 所述的方法。但是，接收机 1300 不对恢复出来的访问码进行验证，并且不基于访问码授权访问。

[0079] 因此，可以将访问码和 / 或密码编码到多个音调中，并从中恢复出来。通过用声音信道输入用于认证的访问码，就不需要显示器或用于显示访问码所需的不断计算，从而延长令牌的电池寿命。此外，由于访问码不是用户手工输入的，所以，不易发生错误，尤其在用户在每次访问期间需要不止一次地输入访问码的系统中。此外，由于可以使用标准的扬声器和 / 或麦克风，所以，可以很容易地实现该系统，而不会明显增加成本。

[0080] 最后，可以通过硬件、软件、固件、中间件、微码或其任意组合来实现实施例。当用软件、固件、中间件或微码来实现时，执行必要任务的程序代码或代码段可以存储在机器可读介质中，如存储介质 210、310、810、1210 或其他存储介质（未显示）。处理器，如处理器 220、230、820 或其他处理器（未显示），可以执行必要的任务。代码段可以代表过程、函数、子程序、程序、例程、子例程、模块、软件包、类或者指令、数据结构或程序表达的任何组合。一个代码段可以通过传送和 / 或接收信息、数据、自变量、参数或存储器内容来与另一代码段或硬件电路相连。信息、自变量、参数、数据等可以通过任何合适的方式来传递、转发或传输，包括存储器共享、消息传递、标记传送、网络传输等。

[0081] 此外，对于本领域技术人员显而易见的是，可以重新排列令牌 200 和 800 的部件，而不影响令牌的操作。同样，可以重新排列验证机设备 300 和 / 或接收机 1200、1300 的部件，而不影响其操作。此外，可以将令牌 200、800、验证机设备 300 和 / 或接收机 1200、1300 的部件实现在一起。例如，可以将处理器 238 与处理器 220 实现在一起，可以将处理器 348 与处理器 320 实现在一起。

[0082] 此外，在有些实施例中，可以用显示器来实现令牌。图 14A 示出的令牌的示例性实施例具有容纳部件 1410，用显示器 1420、致动器 1430 和音频输出单元 1440 来实现。图 18B 示出的令牌的另一示例性实施例具有容纳部件 1450，用显示器 1460、致动器 1470、音频输出单元 1480 和穿过容纳部件 1450 的孔 1480 来实现。

[0083] 因此，前面的实施例只是示例，而不应被解释为限制本发明。对这些实施例的描述是说明性的，而不限制权利要求的保护范围。因此，本申请的内容可以很容易地用于其他类型的装置，并且，各种替换、修改和变化对于本领域技术人员来说是显而易见的。

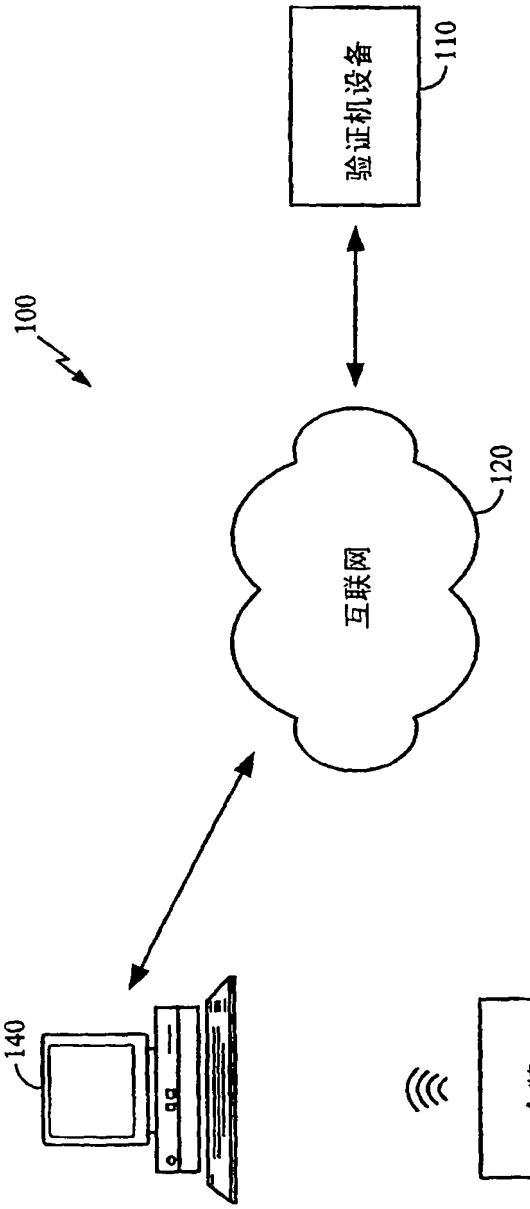


图1

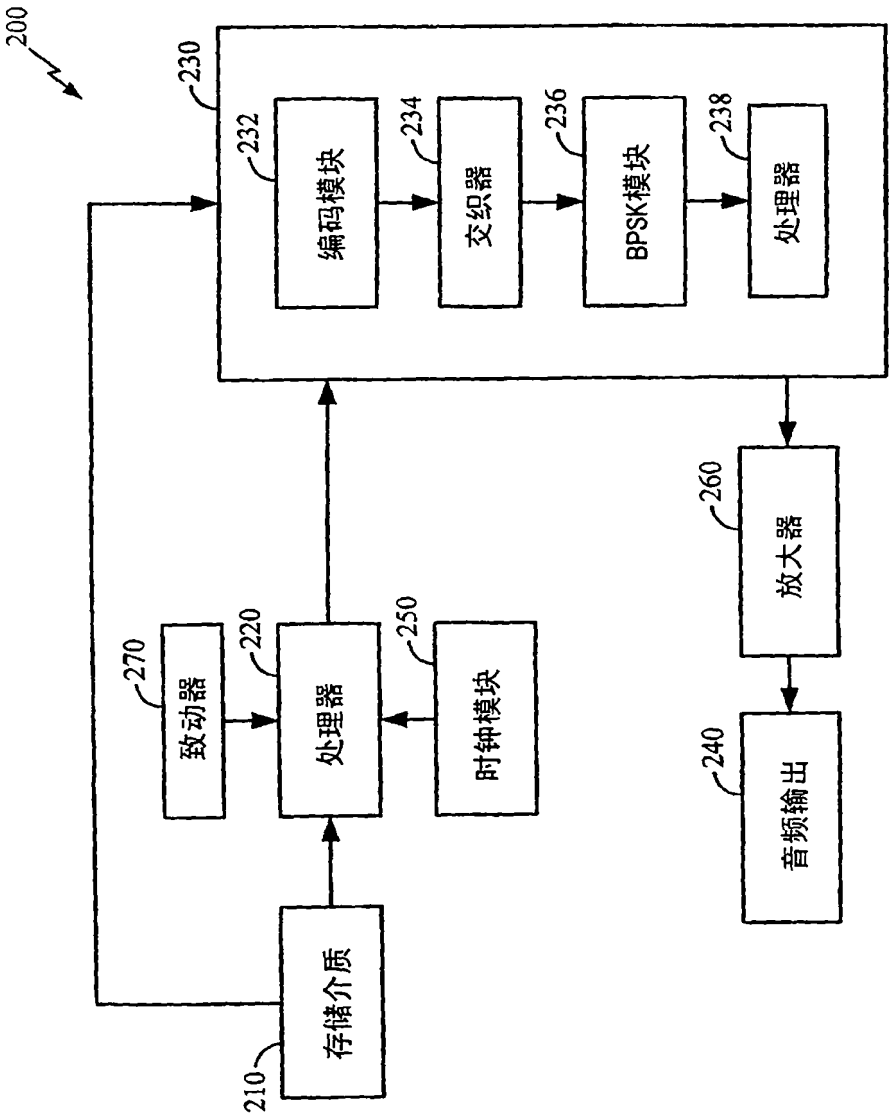

200
230
232
编码模块
234
交织器
236
BPSK模块
238
处理器
260
放大器
240
音频输出
270
致动器
220
处理器
250
时钟模块
210
存储介质

图2

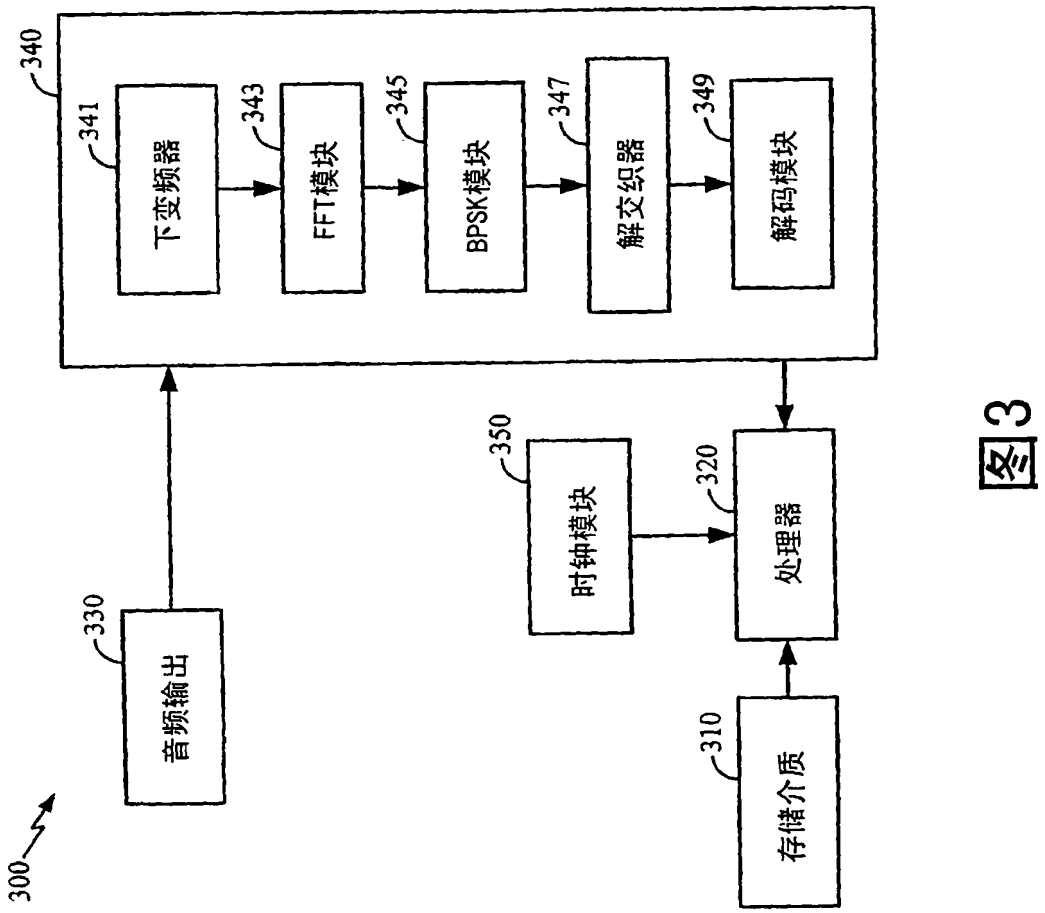

300
340
341
下变频器
343
FFT模块
345
BPSK模块
347
解交织器
349
解码模块
330
音频输出
350
时钟模块
320
处理器
310
存储介质

图3

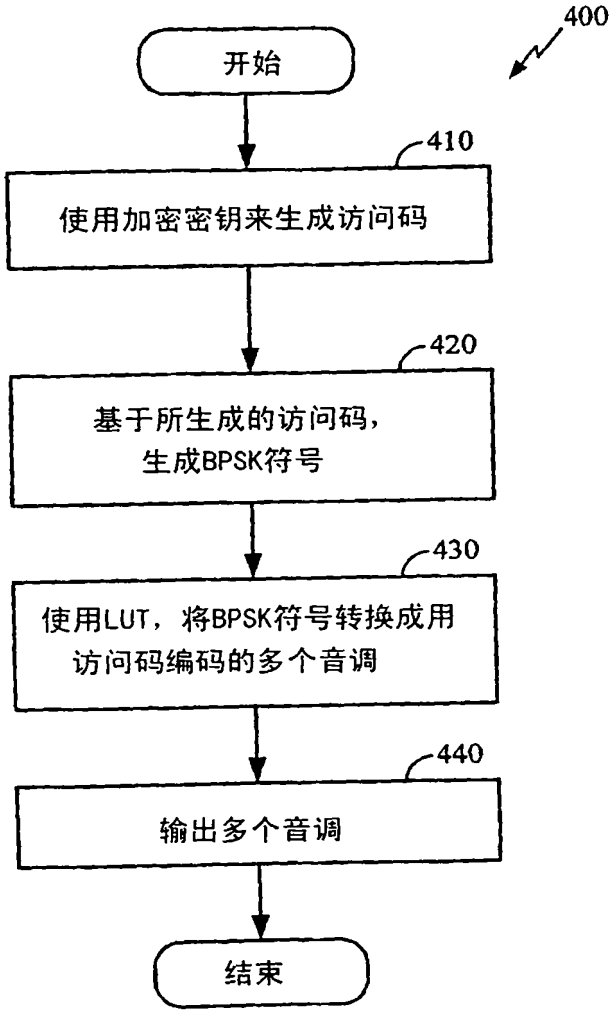


图 4

0	1	1	1	0	0	1	0

BPSK符号

图 5A

0101	1111	0000	1010

重复的BPSK符号

图 5B

T1 000	T2 0001	T3 0010	T4 0011
T5 0100	T6 0101	T7 0110	T8 0111
T9 1000	T10 1001	T11 1010	T12 1011
T13 1100	T14 1101	T15 1110	T16 1111

查找表

图 5C

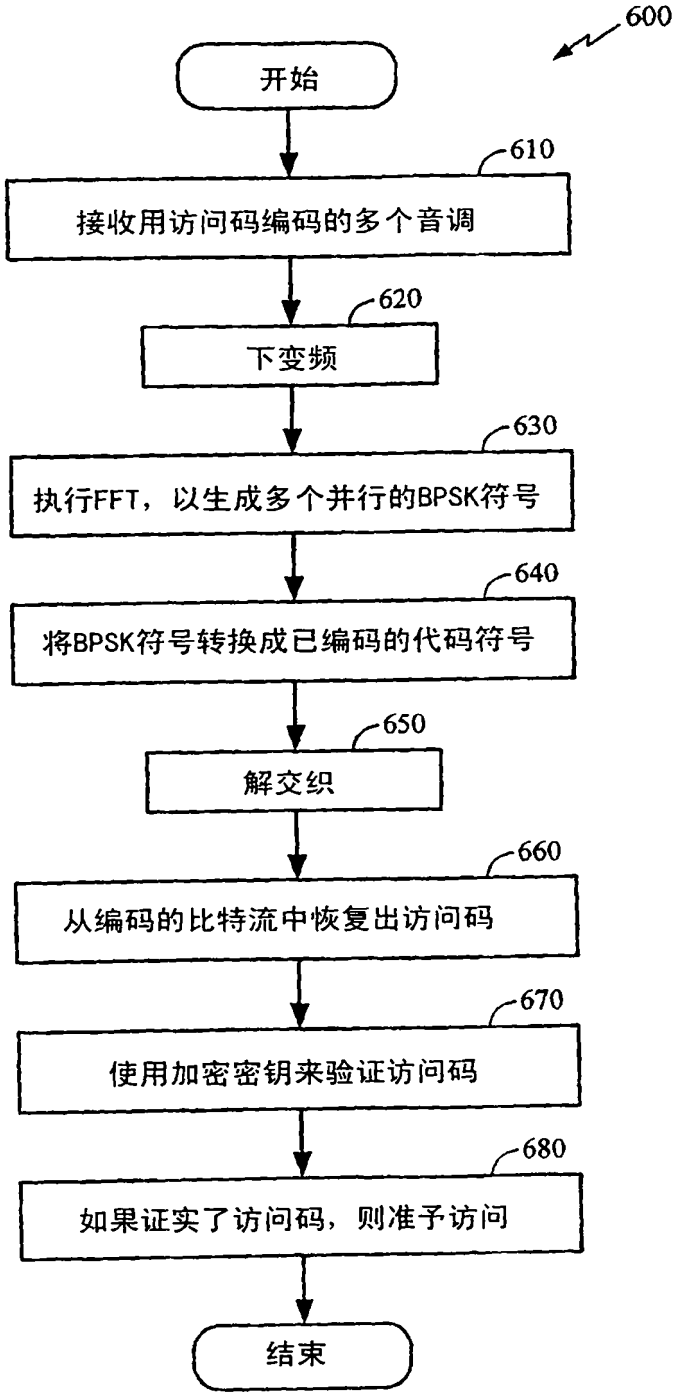

600
开始
610
接收用访问码编码的多个音调
620
下变频
630
执行FFT，以生成多个并行的BPSK符号
640
将BPSK符号转换成已编码的代码符号
650
解交织
660
从编码的比特流中恢复出访问码
670
使用加密密钥来验证访问码
680
如果证实了访问码，则准予访问
结束

图 6

图 7A

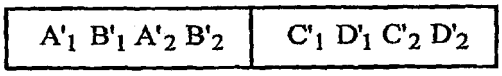


图 7B

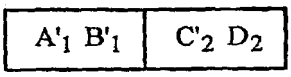


图 7C

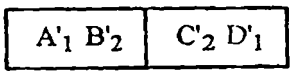


图 7D

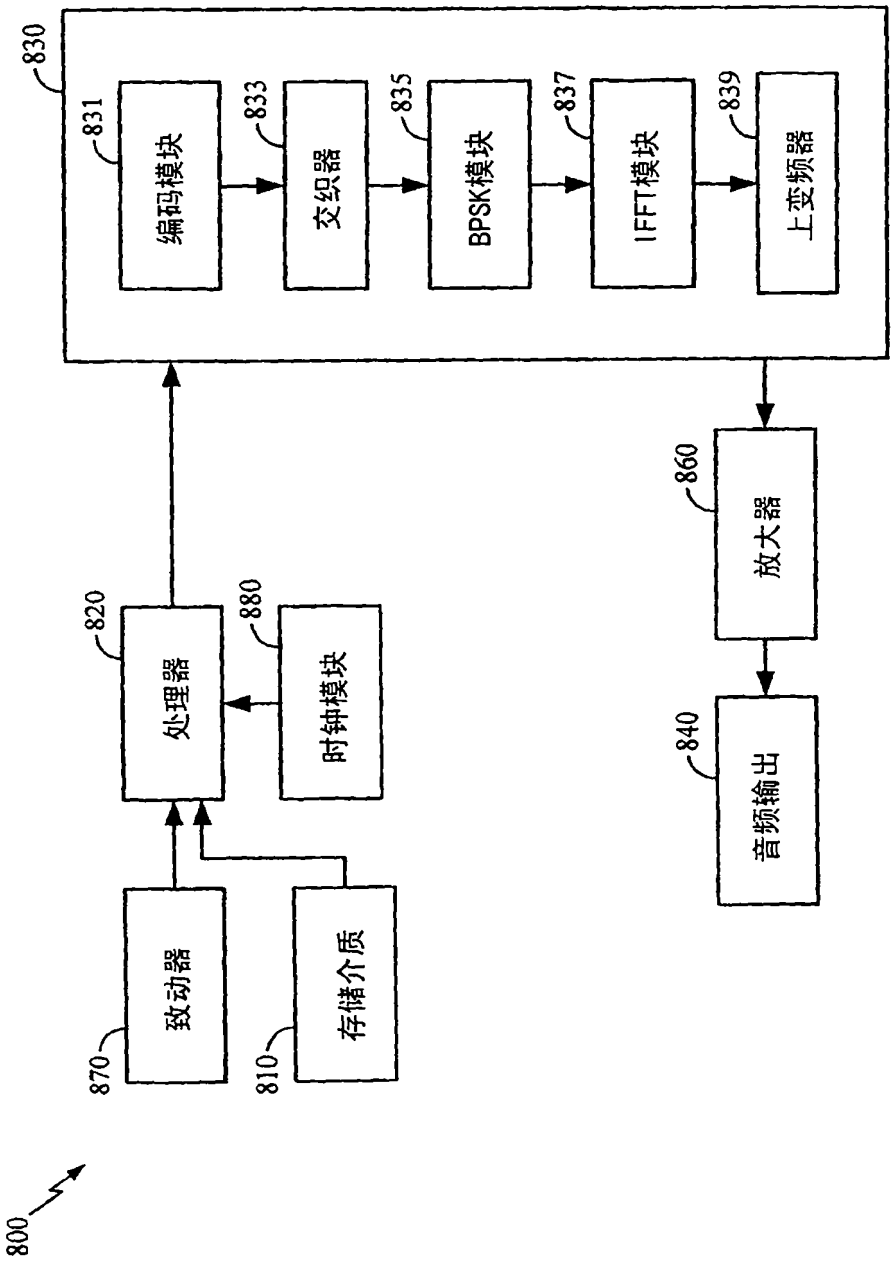

800
830
831
编码模块
833
交织器
835
BPSK模块
837
IFFT模块
839
上变频器
820
处理器
880
时钟模块
860
放大器
840
音频输出
870
致动器
810
存储介质

图8

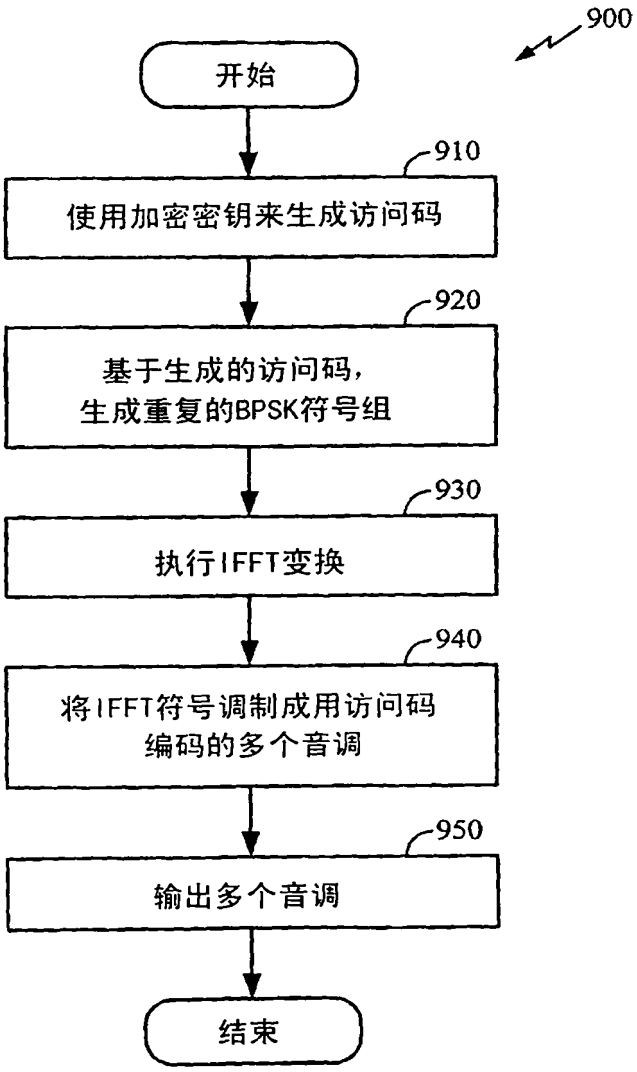

900
开始
910
使用加密密钥来生成访问码
920
基于生成的访问码，
生成重复的BPSK符号组
930
执行IFFT变换
940
将IFFT符号调制成用访问码
编码的多个音调
950
输出多个音调
结束

图 9

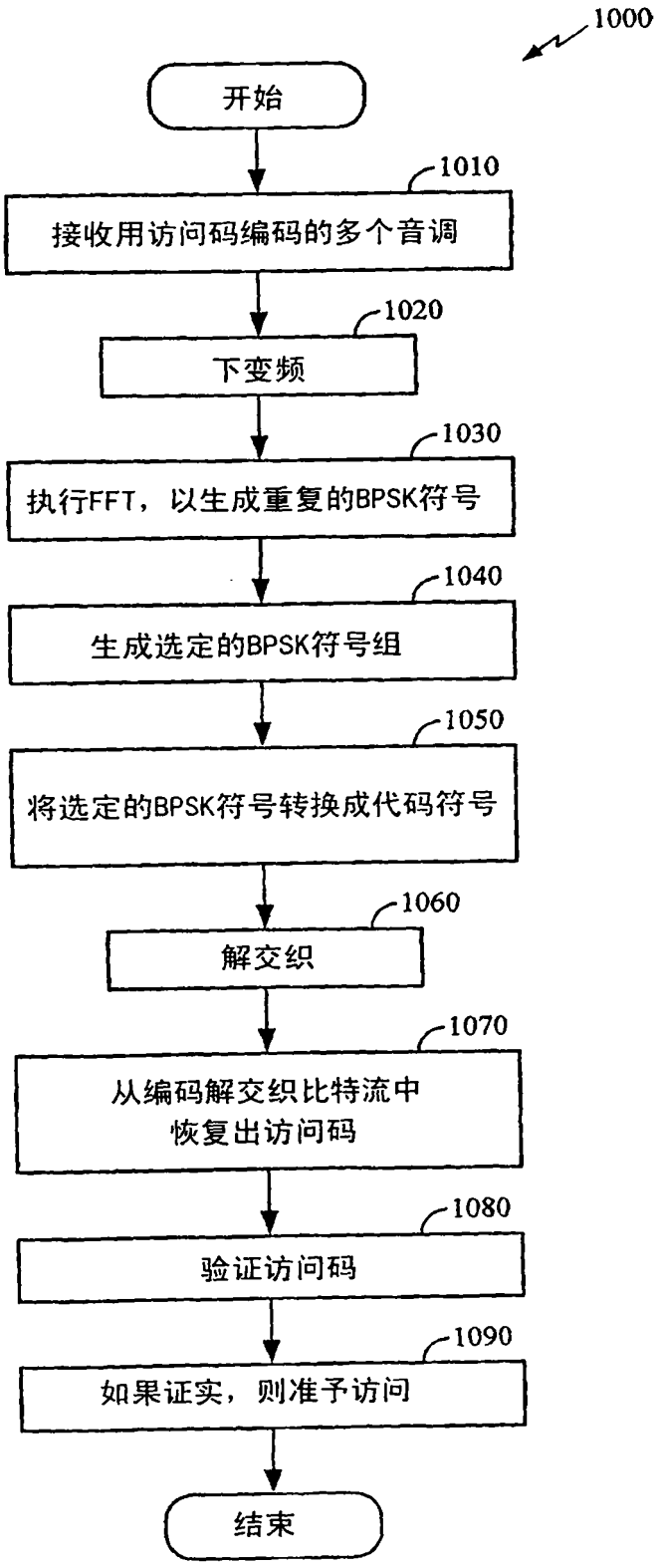

1000
开始
1010
接收用访问码编码的多个音调
1020
下变频
1030
执行FFT，以生成重复的BPSK符号
1040
生成选定的BPSK符号组
1050
将选定的BPSK符号转换成代码符号
1060
解交织
1070
从编码解交织比特流中
恢复出访问码
1080
验证访问码
1090
如果证实，则准予访问
结束

图 10

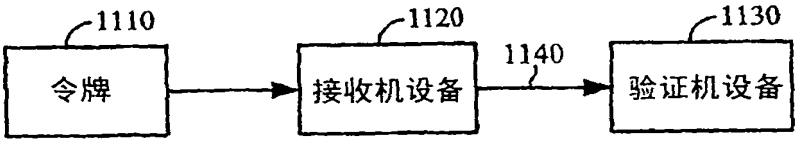


图 11A

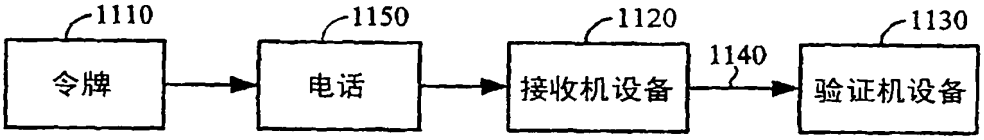


图 11B

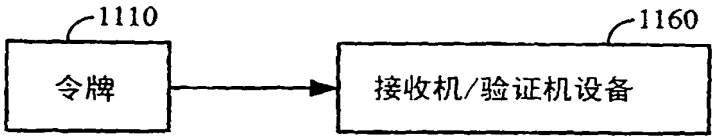


图 11C

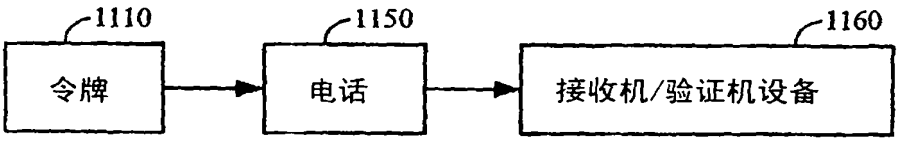


图 11D

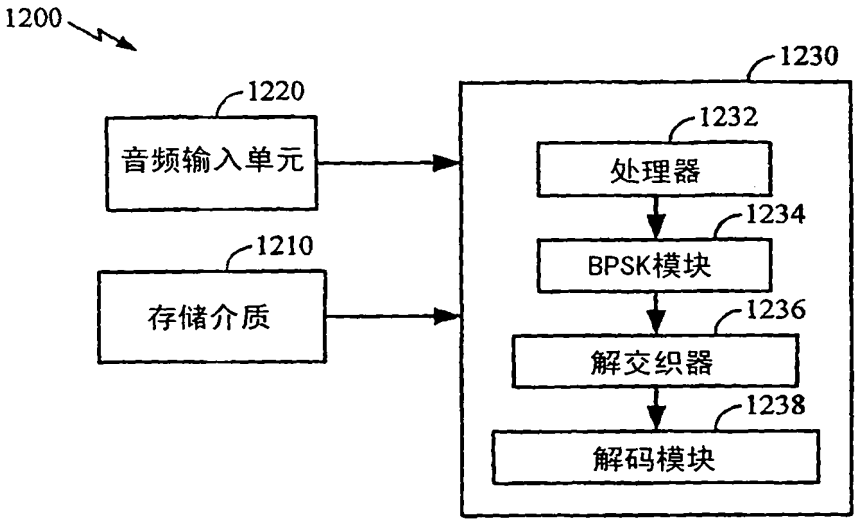

1200
1220
音频输入单元
1210
存储介质
1230
1232
处理器
1234
BPSK模块
1236
解交织器
1238
解码模块

图 12

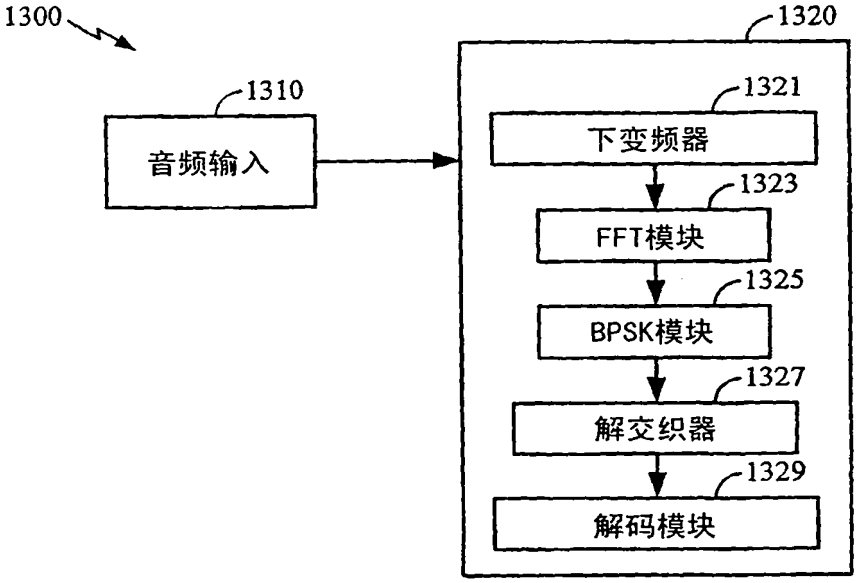

1300
1310
音频输入
1320
1321
下变频器
1323
FFT模块
1325
BPSK模块
1327
解交织器
1329
解码模块

图 13

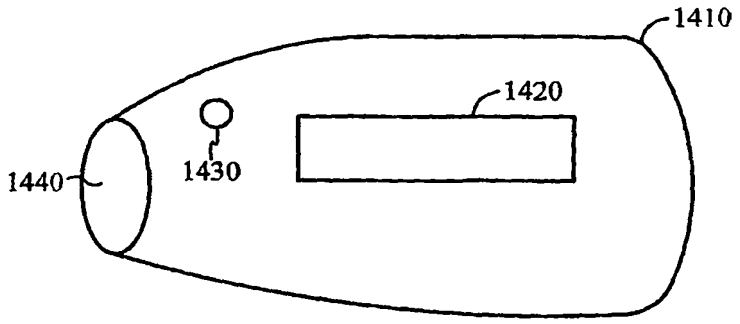


图 14A

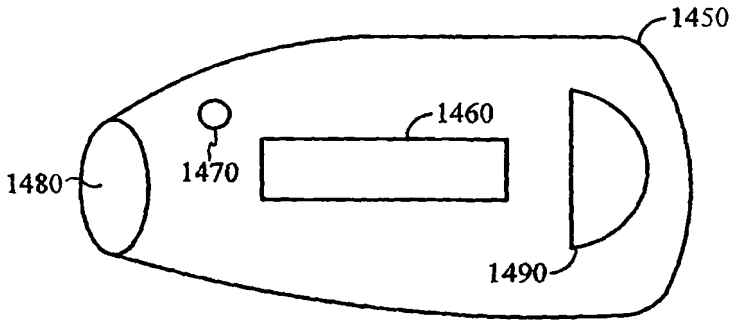


图 14B