(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 108184199 B
(45)授权公告日 2021.06.15

(21)申请号 201711291976.9

(22)申请日 2017.12.08

(65)同一申请的已公布的文献号
申请公布号 CN 108184199 A

(43)申请公布日 2018.06.19

(30)优先权数据
16202916.9 2016.12.08 EP

(73)专利权人 大北欧听力公司
地址 丹麦,巴勒鲁普

(72)发明人 A·M·文德尔伯

(74)专利代理机构 北京尚诚知识产权代理有限公司 11322
代理人 顾小曼

(51)Int.Cl.
H04R 25/00(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 105704113 A,2016.06.22
CN 101989984 A,2011.03.23
US 2005149722 A1,2005.07.07
US 2016094543 A1,2016.03.31
肖跃雷、朱志祥、张勇.一种分析会话密钥分配协议的新方法.《信息处理与网络安全》.2015,
R. Tahir, H. Hu, D. Gu, K. McDonald-Maier and G. Howells.A Scheme for the Generation of Strong ICMetrics Based Session Key Pairs for Secure Embedded System Applications.《2013 27th International Conference on Advanced Information Networking and Applications Workshops》.2013,

审查员 刘畅

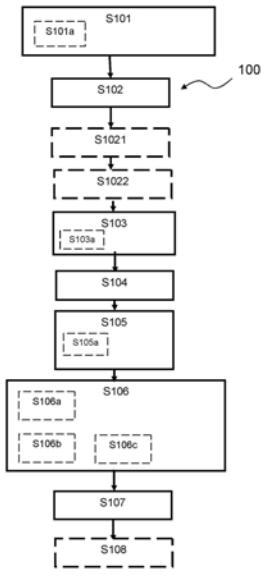
权利要求书2页 说明书13页 附图7页

(54)发明名称

调试设备、服务器设备以及远程配置听力设备的方法

(57)摘要

本发明提供一种在听力系统的调试设备处执行的用于远程配置听力系统中的听力设备的方法。听力系统包括听力设备、调试设备和服务器设备。方法包括获取包括听力设备的听力设备标识符的听力设备数据,以及获取会话密钥。方法包括基于会话密钥和听力设备标识符生成配置发起请求。方法包括将配置发起请求传输到服务器设备;以及从服务器设备接收配置发起响应,所述配置发起响应包括配置密钥材料。方法包括基于听力设备的配置数据并基于配置密钥材料生成配置包,所述配置包包括配置包数据;以及将配置包传输到服务器设备。



CN 108184199 B

1.一种在听力系统的调试设备处执行的用于远程配置所述听力系统中的听力设备的方法,所述听力系统包括所述听力设备、所述调试设备和服务器设备,所述方法包括:

-获取包括所述听力设备的听力设备标识符的听力设备数据;

-获取会话密钥;

-基于所述会话密钥和所述听力设备标识符生成配置发起请求,其中生成所述配置发起请求包括使用配置发起公共秘钥对所述会话密钥进行加密,并且在所述配置发起请求中包括加密的会话密钥;

-将所述配置发起请求传输到所述服务器设备;

-从所述服务器设备接收配置发起响应,所述配置发起响应包括配置密钥材料,其中接收所述配置发起响应包括使用所述会话密钥解密所述配置密钥材料;

-基于所述听力设备的配置数据并基于所述配置密钥材料生成配置包,所述配置包包括配置包数据,其中生成所述配置包包括使用所述配置密钥材料来加密所述配置数据,并且所述配置包数据包括加密的配置数据;以及

-将所述配置包传输到所述服务器设备。

2.根据权利要求1所述的方法,其中所述听力设备数据包括共享索引、调试设备密钥标识符、地址标识符和/或调试信息。

3.根据前述权利要求中任一项所述的方法,其中接收所述配置发起响应包括解密所述配置密钥材料。

4.根据权利要求1所述的方法,其中生成所述配置包包括基于所述配置数据来计算配置数据完整性指示符,并且其中所述配置包数据基于所述配置数据完整性指示符。

5.根据权利要求4所述的方法,其中生成所述配置包包括使用所述配置密钥材料来加密所述配置数据和/或所述配置数据完整性指示符,并且其中所述配置包数据基于加密的配置数据和/或加密的配置数据完整性指示符。

6.根据权利要求4至5中任一项所述的方法,其中所述配置包数据包括配置有效载荷块和控制块,并且其中所述配置有效载荷块包括加密的配置数据和加密的配置数据完整性指示符。

7.根据权利要求1所述的方法,其中生成所述配置包包括加密所述配置包数据。

8.根据权利要求1所述的方法,所述方法包括将访问请求发送到所述服务器设备并从所述服务器设备接收访问响应。

9.根据权利要求1所述的方法,所述方法包括在传输所述配置包之后删除所述会话密钥和所述配置密钥材料。

10.一种在听力系统的服务器设备处执行的用于所述听力系统中的听力设备的远程配置的方法,所述听力系统包括所述听力设备、安装在附属设备上的用户应用、调试设备和所述服务器设备,所述方法包括:

-从所述调试设备接收配置发起请求,所述配置发起请求包括听力设备标识符和会话密钥,使用配置发起公共秘钥对所述会话密钥进行加密;

-使用与所述配置发起公共秘钥对应的配置发起私有秘钥对所述会话密钥进行解密;

-基于所述会话密钥生成配置密钥材料,其中基于所述会话密钥生成所述配置密钥材料包括使用所述会话密钥来加密配置会话密钥,并且将加密的配置会话密钥包括在所述配

置密钥材料中；

-生成配置认证材料；

-将配置发起响应传输到所述调试设备，所述配置发起响应包括所述配置密钥材料；

-从所述调试设备接收配置包，所述配置包包括配置有效载荷块和控制块，其中所述配置有效载荷块包括由所述调试设备使用所述配置密钥材料加密的配置数据；

-基于所述配置有效载荷块和所述控制块计算完整性指示符集；

-基于所述完整性指示符集的至少一部分生成配置块；

-基于所述配置块生成配置验证包；

-基于所述配置认证材料生成配置认证包；以及

-传输所述配置包、所述配置验证包和所述配置认证包。

11.根据权利要求10所述的方法，所述方法包括在所述服务器设备处接收访问请求，所述访问请求包括验配师标识符并将访问响应发送到所述调试设备。

12.根据权利要求10-11中任一项所述的方法，所述方法包括经由所述配置块获取第一数字签名；以及基于所述第一数字签名生成配置验证包。

13.根据权利要求10所述的方法，所述方法包括经由所述配置认证材料获取第二数字签名；并且其中基于所述第二数字签名生成配置认证包。

14.根据权利要求11所述的方法，其中生成所述配置认证材料包括：

-基于所述听力设备标识符获取证书密钥；

-使用所述验配师标识符获取验配师证书；

-使用所述证书密钥加密所述验配师证书；以及

-在所述配置认证材料中包括加密的验配师证书。

15.根据权利要求10所述的方法，其中从所述调试设备接收所述配置包包括使用所述会话密钥来解密所述配置包的配置数据。

16.一种调试设备，包括：

-处理单元；

-存储器单元；以及

-接口；

其中所述调试设备被配置为执行权利要求1-9中的任一项。

17.一种服务器设备，包括：

-处理单元；

-存储器单元；以及

-接口；

其中所述服务器设备被配置为执行权利要求10-15中的任一项。

调试设备、服务器设备以及远程配置听力设备的方法

技术领域

[0001] 本公开涉及一种包括服务器设备、听力设备、调试设备(fitting device)和附属设备的听力系统。特别地,本公开涉及用于通过调试设备、相关调试设备和相关服务器设备来确保听力设备的远程配置的方法。

背景技术

[0002] 随着无线通信技术的发展,去往和来自听力系统的不同实体的无线通信也在不断增加。然而,为了确保听力系统中的通信,新技术为助听器制造商带来新的挑战。听力系统的无线通信接口希望使用基于开放标准的接口。然而,这在安全性方面带来许多挑战。进一步地,听力设备是一种非常小的设备,在计算能力、存储器空间等方面有严格的限制。

发明内容

[0003] 需要调试设备、服务器设备和方法,以用于提供支持听力设备的远程配置的改进和有效的安全性,诸如听力设备的远程调试或远程微调。进一步地,需要减少被第三(未经授权)方损害配置数据的风险的设备和方法。

[0004] 因此,提供了一种在听力系统的调试设备处执行的用于远程配置听力系统中的听力设备的方法。听力系统包括听力设备、调试设备和服务器设备。方法包括获取包括听力设备的听力设备标识符的听力设备数据;以及获取会话密钥。方法包括基于会话密钥和听力设备标识符生成配置发起请求。方法包括将配置发起请求传输到服务器设备;以及从服务器设备接收配置发起响应。配置发起响应包括配置密钥材料。方法包括基于听力设备的配置数据并基于配置密钥材料生成配置包,配置包包括配置包数据;以及将配置包传输到服务器设备。

[0005] 本公开还涉及一种在听力系统的服务器设备处执行的用于听力系统中的听力设备的远程配置的方法。听力系统包括听力设备、安装在附属设备上的用户应用、调试设备和服务器设备。方法包括从调试设备接收配置发起请求,配置发起请求包括听力设备标识符和会话密钥;以及基于会话密钥生成配置密钥材料。方法包括生成配置认证材料;将配置发起响应传输到调试设备,配置发起响应包括配置密钥材料。方法包括从调试设备接收配置包,配置包包括配置有效载荷块和控制块。方法可包括基于配置有效载荷块和控制块计算完整性指示符集。方法可基于完整性指示符集的至少一部分生成配置块。方法包括基于配置块生成配置验证包;以及基于配置认证材料生成配置认证包。方法可包括传输配置包、配置验证包和配置认证包。

[0006] 本公开涉及一种调试设备,包括处理单元、存储器单元以及接口。调试设备被配置为执行根据本公开的方法的步骤中的任一个。

[0007] 本公开涉及一种服务器设备,包括处理单元、存储器单元以及接口。服务器设备被配置为执行根据本公开的方法的步骤中的任一个。

[0008] 本公开的重要优点是提供了听力设备的安全的远程配置,同时考虑了听力设备的

有限计算能力。因此，提供了听力设备的有效和安全的远程配置。

附图说明

[0009] 参考附图通过其示例性实施例的以下详细描述，本发明的上述和其它特征和优点对于本领域技术人员将变得显而易见，其中：

[0010] 图1示意性示出听力系统，

[0011] 图2是根据本公开在调试设备处执行的示例性方法的流程图，

[0012] 图3是根据本公开在服务器设备处执行的示例性方法的流程图，

[0013] 图4示意性示出根据本公开的示例性配置包和示例性配置验证包，

[0014] 图5示意性示出根据本公开的示例性配置认证包，

[0015] 图6示意性示出根据本公开的调试设备、服务器设备、附属设备和听力设备之间的示例性信令图示，

[0016] 图7示意性示出根据本公开的示例性调试设备，以及

[0017] 图8示意性示出根据本公开的示例性服务器设备。

[0018] 附图标记列表：

[0019]	1	听力系统
[0020]	2	调试设备
[0021]	4	服务器设备
[0022]	6	听力设备系统
[0023]	8	听力设备
[0024]	10	附属设备
[0025]	12	用户应用
[0026]	20	用户附属设备和听力设备之间的通信链路
[0027]	21	服务器设备和用户附属设备之间的通信链路
[0028]	22	调试设备和服务器设备之间的通信链路
[0029]	23	调试设备和听力设备系统之间的通信链路
[0030]	24	天线
[0031]	26	无线电收发器
[0032]	28	第一麦克风
[0033]	30	第二麦克风
[0034]	32	处理器
[0035]	32a	确定模块
[0036]	32b	更新模块
[0037]	33	接口
[0038]	34	接收器
[0039]	35	存储器单元
[0040]	36	处理单元
[0041]	36a	确定模块
[0042]	38	存储器单元

[0043]	40	接口
[0044]	100	在调试设备处执行的方法
[0045]	200	在服务器设备处执行的方法
[0046]	301	存储器单元
[0047]	302	处理单元
[0048]	302a	获取模块
[0049]	302b	生成模块
[0050]	302c	删除模块
[0051]	303	接口
[0052]	402	配置包
[0053]	403	配置包数据
[0054]	404	配置有效载荷块
[0055]	406	配置控制块
[0056]	408	配置数据
[0057]	409	配置数据完整性指示符
[0058]	412	配置验证包
[0059]	414	第一完整性指示符
[0060]	416	第二完整性指示符
[0061]	418	第一数字签名
[0062]	419	配置块
[0063]	502	配置认证包
[0064]	504	配置认证材料
[0065]	506	验配师证书
[0066]	508	第二数字签名
[0067]	600	信令图示
[0068]	601	访问请求
[0069]	602	访问响应
[0070]	604	配置发起请求
[0071]	606	配置发起响应
[0072]	608	配置包
[0073]	610	配置验证包
[0074]	612	配置认证包
[0075]	614	消息
[0076]	616	消息
[0077]	618	消息
[0078]	801	存储器单元
[0079]	802	处理单元
[0080]	802a	生成模块
[0081]	802b	获取模块

[0082] 803 接口

[0083] 804 安全模块。

具体实施方式

[0084] 下文在适当时参考附图描述各种示例性实施例和细节。应当注意，附图可以或可以不按比例绘制，并且在整个附图中，相似结构或功能的元件由相同的附图标记表示。还应当注意，附图仅旨在促进对实施例的描述。它们不旨在作为对本发明的详尽描述或作为对本发明的范围的限定。另外，所示出的实施例不需要具有示出的所有方面或优点。结合特定实施例描述的方面或优点不必然地局限于该实施例，并且可以在任何实施例中实践，即使不是如此示出，或者如果不是如此明确描述的那样。

[0085] 本公开涉及远程配置听力系统中的听力设备时的改进安全性。听力系统包括服务器设备、听力设备和调试设备。调试设备由验配师(dispenser)控制。服务器设备可由听力设备制造商控制。服务器设备可以是分布式服务器设备，即具有分布式处理器的服务器设备。也就是说，本文公开的方法、调试设备和服务器设备能够通过调试实现听力设备的远程配置，其中远程配置通过实施适当的保护措施和对策(诸如安全机制)而对安全威胁、漏洞和攻击产生鲁棒性，以便防止威胁和攻击。本公开涉及一种用于远程配置听力设备的方法，其对于重播攻击、未经授权的访问、电池耗尽攻击和中间人攻击具有鲁棒性。

[0086] 本公开解决了验配师和听力设备用户遇到的问题。这可以在以下示例中说明。听力设备用户(例如，从家中)给验配师打电话，并针对早先在专业验配师的办公室完成的配置或调试提出诉求。验配师应该能够在办公室中调整某些配置值(例如，1kHz的+3db增益)，并将所得到的配置包或微调包发送到听力设备或其上安装有应用程序的配件，以对听力设备进行处理。听力设备用户能够使用应用以下载配置包并将其应用于听力设备。然而，配置包的这种检索应该被保护，配置包的完整性应该被保护，并且导致在听力设备上安调试置包的整个处理链将被保密、认证和进行完整性保护。

[0087] 调试设备包括分别连接到处理单元的存储器单元和接口。存储器单元可以包括可移除和不可移除数据存储单元，包括但不限于只读存储器(ROM)、随机存取存储器(RAM)等。调试设备被配置为控制和/或配置听力设备。接口包括天线和无线收发器，例如，配置为在2.4GHz至2.5GHz范围内的频率下进行无线通信。接口可以被配置用于通信，诸如无线通信，其中听力设备包括天线和无线收发器以及服务器设备。

[0088] 本公开涉及听力系统的实体之间的听力系统通信。附属设备形成到听力设备的附属设备。附属设备通常配对或以其他方式无线耦合到听力设备。听力设备可以是助听器，例如耳背式(BTE)类型、耳内(ITE)类型、耳道内(ITC)类型、耳道内接收器(RIC)类型或耳内接收器(RITE)类型。通常，听力设备系统由听力设备用户掌握和控制。附属设备可以是智能电话、智能手表或平板计算机。

[0089] 如本文所使用的术语“标识符”是指用于识别(诸如用于分类和/或唯一识别)的数据片段。标识符可以是字、数字、字母、符号、列表、数组或其任何组合的形式。例如，作为数字的标识符可以是整数的形式，诸如具有一定长度或以上的无符号整数uint，诸如无符号整数的数组。标识符可具有若干个字节的长度。例如，听力设备标识符可以具有10-30字节的长度，诸如20字节。

[0090] 本公开涉及一种在听力系统的调试设备处执行的方法。提供了用于在听力系统中远程配置听力设备的方法，听力系统包括听力设备、配件设备和服务器设备。方法包括获取听力设备数据。听力设备数据包括将由调试设备远程配置的听力设备的听力设备标识符。在一个或多个示例性方法中，获取听力设备数据包括从远离调试设备的数据库获取或检索听力设备数据。听力设备数据包括听力设备的听力设备标识符。听力设备标识符可以指唯一的设备标识符。听力设备标识符可以包括硬件号、序列号、MAC地址。在一个或多个示例性方法中，听力设备数据可以包括共享索引、调试设备密钥标识符、地址标识符(诸如蓝牙地址)和/或调试信息。共享索引可以支持识别与听力设备共享的公密，从而提供有效载荷的使用的优化。地址标识符可以具有2-10字节的长度，诸如5字节，诸如6字节。共享索引可具有1字节的长度。调试设备密钥标识符可以具有1字节到3字节之间的长度，诸如2字节。

[0091] 一个或多个示例性方法包括获取会话密钥。获取会话密钥可以包括生成会话密钥，例如，作为随机数或伪随机数。可以为每个会话唯一地生成会话密钥。会话密钥可以是对称密钥。对称会话密钥可以提供处理单元上的安全算法的轻量级处理，诸如轻量级加密、轻量级解密、轻量级完整性保护等。会话密钥可以具有10字节和20字节之间的长度，诸如15字节和20字节之间，诸如16字节。

[0092] 一个或多个示例性方法包括获取会话计数器。获取会话计数器可以包括生成会话计数器，例如作为随机数或伪随机数。会话计数器可以具有10字节和20字节之间的长度，诸如在15字节和20字节之间，诸如16字节。

[0093] 一个或多个示例性方法包括基于会话密钥和听力设备标识符生成配置发起请求。例如，生成配置发起请求可以包括使用配置发起公共秘钥加密会话密钥，并且在配置发起请求中包括加密的会话密钥。在一个或多个示例性方法中，生成配置发起请求可以包括通过例如使用配置发起公共秘钥来加密会话密钥、会话计数器和听力设备数据的一部分(例如，共享索引、调试设备密钥标识符)来加密会话密钥和会话计数器。加密可以基于RSA密码系统或任何其他加密系统。

[0094] 一种或多种示例性方法包括将配置发起请求传输到服务器设备。配置发起请求可以包括会话密钥、听力设备标识符以及可选地听力设备数据的一部分(例如，共享索引)，以及可选地会话计数器。可以在传输之前使用配置发起公共秘钥加密配置发起请求。

[0095] 一个或多个示例性方法包括从服务器设备接收配置发起响应，该配置发起响应包括配置密钥材料。在一个或多个示例性方法中，接收配置发起响应包括解密配置密钥材料。例如，可以使用会话密钥解密配置密钥材料。配置密钥材料可以包括配置密钥(诸如对称)，以及可能包括配置密钥计数器。

[0096] 一个或多个示例性方法包括基于听力设备的配置数据并基于配置密钥材料来生成配置包。配置包可以包括配置包数据。配置数据可以包括与听力设备相关的数据。与听力设备相关的数据可以包括听力设备设置和/或调试参数。

[0097] 在一个或多个示例性方法中，生成配置包包括基于配置数据来计算配置数据完整性指示符。配置包数据可以基于配置数据完整性指示符。配置包数据可以包括配置数据完整性指示符。配置数据完整性指示符CDI可以指代使接收方能够验证数据的完整性的指示符，所述CDI附加到所述数据。CDI可以包括例如散列校验和，诸如基于散列函数的校验和，诸如SHA函数，例如，SHA1、SHA2。例如，可以使用散列函数来执行基于配置数据计算配置数

据完整性指示符。

[0098] 在一个或多个示例性方法中，生成配置包包括使用配置密钥材料来加密配置数据和/或配置数据完整性指示符。配置包数据可以基于加密的配置数据和/或加密的配置数据完整性指示符。例如，配置包数据可以包括加密的配置数据和/或加密的配置数据完整性指示符。

[0099] 在一个或多个示例性方法中，配置包数据可以包括配置有效载荷块和控制块，并且配置有效载荷块可以包括加密的配置数据和加密的配置数据完整性指示符。控制块是例如元数据，诸如配置数据的头部、CDI、长度。

[0100] 在一个或多个示例性方法中，生成配置包包括加密配置包数据，例如，使用会话秘钥。换句话说，配置包数据包括加密的配置数据和/或加密的配置数据完整性指示符，和/或使用会话密钥的控制块。

[0101] 一个或多个示例性方法包括将配置包传输到服务器设备。一个或多个示例性方法可以包括在传输配置包之后删除会话密钥和配置密钥材料。

[0102] 在一个或多个示例性方法中，方法可以包括将访问请求发送到服务器设备并从服务器设备接收访问响应。例如，调试设备可以基于登录和密码发送访问请求，并且基于登录和密码的验证来接收访问响应。可以执行向服务器设备发送访问请求并从服务器设备接收访问响应，以获取对服务器设备的访问以进行通信(例如，配置发起请求和配置包)。

[0103] 本公开涉及在听力系统的服务器设备处执行的用于在听力系统中远程配置听力设备的方法。听力系统包括听力设备、安装在附属设备上的用户应用、调试设备和服务器设备。服务设备可以包括安全模块，其中安全模块被配置为执行安全操作，诸如导出密钥、加密证书、数字签名。安全模块可以被实现为硬件安全模块，其与服务器设备并置或远程。附属设备上安装有用户应用。

[0104] 附属设备包括分别连接到处理单元的存储器单元和接口。存储器单元具有存储在其上的用户应用。用户应用可以是听力设备应用，例如被配置为与听力设备无线通信，诸如用于控制和/或配置听力设备。接口包括天线和无线收发器，例如，被配置为在2.4GHz至2.5GHz范围内的频率下进行无线通信。接口可以被配置用于通信，诸如无线通信，其中听力设备包括天线和无线收发器。附属设备形成到听力设备的附属设备。附属设备通常配对或以其他方式无线耦合到听力设备。听力设备可以是助听器，例如耳背式(BTE)类型、耳内(ITE)类型、耳道内(ITC)类型、耳道内接收器(RIC)类型或耳内接收器(RITE)类型。通常，附属设备由听力设备用户拥有并控制。附属设备可以是手持设备，诸如智能电话或平板计算机，或诸如智能手表的可穿戴设备。

[0105] 在服务器设备处执行的一个或多个示例性方法包括从调试设备接收配置发起请求。配置发起请求可以包括听力设备标识符和/或会话密钥。可以使用配置发起公共秘钥以加密形式在服务器设备处接收会话密钥。方法可然后包括使用相应配置发起私有秘钥来解密会话密钥。配置发起请求可以包括会话计数器。

[0106] 在服务器设备处执行的一个或多个示例性方法包括基于会话密钥生成配置密钥材料。配置密钥材料可以包括配置密钥和/或配置计数器，两者都可以是明文或使用会话密钥的加密形式。在服务器设备处执行的一个或多个示例性方法包括向调试设备传输配置发起响应。配置发起响应包括配置密钥材料。

[0107] 在服务器设备处执行的一个或多个示例性方法包括生成配置认证材料。在服务器设备执行的一个或多个示例性方法中，方法可以包括在服务器设备处接收访问请求，并将访问响应发送到调试设备。访问请求可以包括验配师标识符。验配师标识符可以是唯一标识符，所述唯一标识符被分配给操作调试设备的验配师或一组验配师。验配师标识符被配置为在服务器设备的存储器模块或数据库中查找验配师证书时支持服务器设备。

[0108] 在一个或多个示例性方法中，生成配置认证材料包括基于听力设备标识符获取证书密钥；使用验配师标识符获取验配师证书；使用证书密钥加密验配师证书；并将加密的验配师证书包括在配置认证材料中。例如，基于听力设备标识符获取证书密钥可以包括从服务器设备的存储器模块检索公共秘钥，或者计算作为散列函数的输出的证书密钥，所述散列函数将字符串和公共秘钥作为输入。使用验配师标识符获取验配师证书可以包括基于验配师标识符识别或检索验配师证书。配置认证材料可以包括用于将材料识别为配置认证材料的类型标识符、指示何时生成配置认证材料的时间戳、被配置为将配置认证材料链接到配置密钥材料的链接标识符、对应于所述配置被寻址的听力设备的听力设备标识符、听力设备的地址标识符、配置认证材料的长度、质询材料、索引、密钥标识符和/或包括加密的验配师证书。

[0109] 在服务器设备处执行的一个或多个示例性方法包括将配置发起响应传输到调试设备，所述配置发起响应包括配置密钥材料。

[0110] 在服务器设备处执行的一个或多个示例性方法包括从调试设备接收配置包。配置包可以包括配置有效载荷块和控制块(诸如元数据，例如头部和一个或多个校验和)。配置有效载荷块可以包括配置数据和配置数据完整性指示符。在一个或多个示例性方法中，从调试设备接收配置包可以包括使用会话密钥解密配置包数据。

[0111] 在服务器设备处执行的一个或多个示例性方法包括基于配置有效载荷块和控制块计算完整性指示符集。完整性指示符集可以包括一个或多个完整性指示符，诸如第一完整性指示符、第二完整性指示符。例如，方法可以包括基于配置有效载荷块来计算第一完整性指示符和基于控制块计算第二完整性指示符。在服务器设备处执行的一个或多个示例性方法包括基于完整性指示符集的至少一部分来生成配置块。配置块可以包括块类型标识符、时间戳、块标识符、听力设备的听力设备标识符、地址标识符、第一完整性指示符和/或第二完整性指示符。

[0112] 在服务器设备处执行的一个或多个示例性方法包括基于配置块生成配置验证包。在一个或多个示例性方法中，方法可以包括通过配置块获取第一数字签名；并且基于第一数字签名生成配置验证包。例如，服务器设备可以被配置为基于配置块和配置私有秘钥生成第一数字签名，或者从安全模块获取第一数字签名。基于第一数字签名生成配置验证包可以包括在配置验证包中包括第一数字签名。

[0113] 在服务器设备处执行的一个或多个示例性方法包括基于配置认证材料生成配置认证包。在一个或多个示例性方法中，方法可以包括通过配置认证材料获取第二数字签名；并且基于第二签名生成配置认证包。例如，服务器设备可以被配置为基于配置认证材料和配置私有秘钥生成第二数字签名，或者从安全模块获取第二数字签名。基于第二数字签名生成配置认证包可以包括在配置认证包中包括第二数字签名。生成配置认证包，使得听力设备可以验证配置数据的完整性。

[0114] 在服务器设备处执行的一个或多个示例性方法包括经由附属设备和可能地经由安装在其上的应用程序将配置包、配置验证包和配置认证包(诸如到附属设备)传输到安装在附属设备上的应用程序,或者传输到听力设备。

[0115] 在附属设备处使用配置验证包来验证配置包和/或配置认证包。在听力设备处使用配置认证包以认证实际上包括将安装在听力设备上的调试参数或配置数据的配置包。换句话说,验配师或调试设备使用服务器设备来创建用于特定听力设备的配置认证包。生成配置认证包和配置包中的配置包数据,使得听力设备能够验证配置包来自合法验配师或合法调试设备,并且配置包中的配置数据未被篡改也未被任何其他方公开,这是因为配置数据是可用于对听力设备上的服务攻击或电池耗尽攻击执行拒绝的私有数据。

[0116] 本公开涉及包括处理单元、存储器单元和接口的调试设备。调试设备被配置为执行根据本公开的方法的步骤中的任一个。

[0117] 本公开涉及包括处理单元、存储器单元和接口的服务器设备。服务器设备被配置为执行根据本公开的方法的步骤中的任一个。

[0118] 为了清楚起见,这些附图是示意性的和简化的,并且它们仅仅示出支持本公开的细节,而其余的细节已经被省略。在整个过程中,相同的附图标记用于相同或相应的部分。

[0119] 图1示出示例性听力系统1。听力系统1包括服务器设备4、调试设备2以及包括听力设备8和附属设备10的听力设备系统6。附属设备10是手持设备,诸如被配置为与听力设备8进行无线通信的智能电话。用户应用12安装在附属设备10上。用户应用可以用于控制听力设备8和/或辅助听力设备用户佩戴/使用听力设备8。在一个或多个示例性用户应用中,用户应用12被配置为将配置数据(例如,听力设备设置或调试参数)传送到听力设备。附属设备10包括处理单元36、存储器单元38和接口40。

[0120] 听力设备8包括天线24以及耦合到天线24的无线电收发器26,以用于接收/传输包括第一通信链路20的无线通信。听力设备8包括一组麦克风,其包括第一麦克风28和可选地第二麦克风30,以用于提供相应的第一和第二麦克风输入信号。听力设备8可以是单麦克风听力设备。听力设备8包括连接到处理器32的存储器单元(未示出),其中配置数据,例如,调试或听力设备设置存储在存储器单元中。

[0121] 听力设备8包括连接到收发器26的处理器32以及用于接收和处理输入信号的麦克风28、30。处理器32被配置为基于听力设备设置补偿用户的听力损失,并且基于输入信号提供电输出信号。接收器34将电输出信号转换成音频输出信号以指向听力设备用户的耳膜。

[0122] 调试设备2能够通过通信链路22与服务器设备4通信,并且通过通信链路23与听力设备系统6通信。听力设备8能够通过通信链路20与附属设备10通信。在实施例中,调试设备2被配置用于经由通信链路23与附属设备10进行通信,并且助听器设备被配置用于经由通信链路20与附属设备10通信。

[0123] 在一个实施例中,服务器设备4被配置为经由通信链路21与听力设备系统6(诸如与附属设备10和/或可选地与听力设备8)进行通信。

[0124] 图2示出根据本公开在调试设备(诸如图1的调试设备2)处执行的示例性方法100的流程图。图2示出用于远程配置听力系统中的听力设备(诸如图1的听力设备8)的方法100,所述听力系统包括听力设备8、附属设备10、调试设备(诸如图1的调试设备2)和服务器设备(诸如图1的服务器设备4)。方法100包括获取S101听力设备数据。听力设备数据包括听

力设备标识符。在一个或多个示例性方法中，获取听力设备数据包括经由通信链路22从远离调试设备诸如远离服务器设备4的数据库获取S101a或检索听力设备数据。方法100包括获取S102会话密钥。获取S102会话密钥可以包括生成会话密钥，例如作为随机数或伪随机数。方法100包括基于会话密钥和听力设备标识符生成S103配置发起请求。例如，生成S103配置发起请求可以包括使用配置发起公共秘钥加密S103a会话密钥，并且在配置发起请求中包括加密的会话密钥。方法100包括例如经由通信链路22将配置发起请求传输S104到服务器设备。配置发起请求包括会话密钥、听力设备标识符、可选地听力设备数据的一部分(例如，共享索引)，以及可选地会话计数器。在传输之前使用配置发起公共秘钥加密配置发起请求。

[0125] 方法100包括例如经由通信链路22从服务器设备接收S105配置发起响应，所述配置发起响应包括配置密钥材料。接收S105配置发起响应可以包括解密S105a配置密钥材料。例如，使用会话密钥解密配置密钥材料。配置密钥材料可以包括配置密钥(诸如对称密钥)，以及可能地包括配置密钥计数器。

[0126] 方法100包括基于听力设备的配置数据并基于配置密钥材料生成S106配置包。配置包包括配置包数据。配置数据可以包括与听力设备相关的数据。与听力设备相关的数据可以包括听力设备设置和/或调试参数。

[0127] 在一个或多个示例性方法中，生成S106配置包包括基于配置数据计算S106a配置数据完整性指示符。配置包数据可以基于配置数据完整性指示符。在一个或多个示例性方法中，生成S106配置包包括使用配置密钥材料来加密S106b配置数据和/或配置数据完整性指示符。配置包数据可以基于加密的配置数据和/或加密的配置数据完整性指示符。例如，配置包数据可以包括加密的配置数据和/或加密的配置数据完整性指示符。在一个或多个示例性方法中，生成S106配置包包括例如使用会话秘钥加密S106c配置包数据。

[0128] 方法100包括例如经由通信链路22将配置包传输S107到服务器设备。一个或多个示例性方法100可以包括在传输配置包之后删除S108会话密钥和配置密钥材料。

[0129] 在一个或多个示例性方法中，方法100可以包括例如经由通信链路22将访问请求发送S1021到服务器设备，以及例如经由通信链路22从服务器设备接收S1022访问响应。例如，调试设备可以基于登录和密码发送访问请求，并且基于登录和密码的验证来接收访问响应。可以执行向服务器设备发送访问请求并从服务器设备接收访问响应，以获取对服务器设备的访问以进行通信(例如，配置发起请求和配置包)。

[0130] 图3示出根据本公开在服务器设备(诸如图1的服务器设备4)执行的示例性方法200的流程图。图3示出用于在听力系统中远程配置听力设备的方法200，诸如用于在执行听力设备的安全远程配置时支持调试设备。听力系统包括听力设备、安装在附属设备上的用户应用、调试设备和服务器设备。

[0131] 方法200包括例如经由通信链路22从调试设备接收S201配置发起请求。配置发起请求包括听力设备标识符和/或会话密钥。可以使用配置发起公共秘钥以加密形式在服务器设备处接收会话密钥。方法200可以包括使用相应配置发起私有秘钥来解密会话密钥。配置发起请求可以包括会话计数器。

[0132] 方法200包括基于会话密钥生成S202配置密钥材料。配置密钥材料可以包括配置密钥和/或配置计数器，两者都可以是明文或使用会话密钥的加密形式。方法200包括例如

经由通信链路22将配置发起响应传输到调试设备。配置发起响应包括配置秘钥材料。

[0133] 方法200包括生成S203配置认证材料。在服务器设备处执行的一个或多个示例性方法中，方法200可以包括在服务器设备处接收S2021访问请求，以及将访问响应发送S2022到调试设备。访问请求包括验配师标识符。在一个或多个示例性方法中，方法200包括生成S203配置认证材料；包括基于听力设备标识符获取S203a证书密钥；使用验配师标识符获取S203b验配师证书；使用证书密钥加密S203c验配师证书；并在配置认证材料中包括S203d加密的验配师证书。例如，基于听力设备标识符获取S203a证书密钥可以包括从服务器设备的存储器模块中检索公共秘钥，或者计算作为散列函数的输出的证书密钥，所述散列函数将字符串和公共秘钥作为输入。使用验配师标识符获取S203b验配师证书可以包括基于验配师标识符识别或检索验配师证书。

[0134] 方法200包括例如经由通信链路22将配置发起响应传输S204到调试设备，所述配置发起响应包括配置密钥材料。方法200包括例如经由通信链路22从调试设备接收S205配置包。配置包包括配置有效载荷块和控制块(诸如元数据，例如头部和一个或多个校验和)。配置有效载荷块可以包括配置数据和配置数据完整性指示符。在一个或多个示例性方法中，从调试设备接收S205配置包可以包括使用会话密钥解密S205a配置包数据。

[0135] 方法200包括基于配置有效载荷块和控制块计算S206完整性指示符集。完整性指示符集可以包括一个或多个完整性指示符，每个完整性指示符是基于配置包的一个或多个部分计算的。例如，方法200可以包括基于配置有效载荷块来计算第一完整性指示符和基于控制块计算第二完整性指示符。方法200包括基于完整性指示符集的至少一部分来生成S207配置块。配置块可以包括第一完整性指示符和/或第二完整性指示符，以及可选地块类型标识符、时间戳、块标识符、听力设备的听力设备标识符和地址标识符中的任一个。

[0136] 方法200包括基于配置块生成S208配置验证包。方法200可以包括通过配置块获取S2071第一数字签名，并且基于第一数字签名生成配置验证包。例如，获取S2071第一数字签名包括基于配置块和配置私有秘钥生成第一数字签名，或者从安全模块获取第一数字签名。生成S208配置验证包可以包括在配置验证包中包括第一数字签名。

[0137] 方法200包括基于配置认证材料生成S209配置认证包。方法200可以包括通过配置认证材料获取S2081第二数字签名；并且基于第二签名生成配置认证包。例如，获取S2081第二数字签名包括基于配置认证材料和配置私有秘钥生成第二数字签名，或者从安全模块获取第二数字签名。基于第二数字签名生成配置认证包可以包括在配置认证包中包括第二数字签名。

[0138] 方法200包括经由附属设备和可能地经由安装在其上的应用程序将配置包、配置验证包和配置认证包(诸如到附属设备)传输S210到安装在附属设备上的应用程序，或者传输到听力设备。例如，方法200可以包括经由通信链路23将配置包、配置验证包和配置认证包传输S210到附属设备10，传输到安装12在附属设备10上的应用程序。在一个或多个示例性实施例中，方法200可包括经由通信链路23和20通过附属设备10将配置包和配置认证包传输S210到听力设备8.

[0139] 图4示意性示出根据本公开的示例性配置包402和示例性配置验证包412。配置包402包括配置包数据403。配置包数据403包括配置有效载荷块404和控制块406。基于听力设备的配置数据408生成配置包402。配置包数据403包括配置数据408，其是用于配置听力设

备的实际调试参数或听力设备设置参数。配置数据408可以使用包括配置密钥的配置密钥材料以加密形式包括在配置包数据403中。配置包数据403包括在配置数据408上计算并被包括在配置包数据403中的配置数据完整性指示符409。配置有效载荷块404包括配置数据408和配置数据完整性指示符409，其可选地为加密形式，如图4中的虚线框指示。控制块406包括头部、配置数据和元数据的长度。调试设备可以被配置为通过例如使用会话秘钥来加密配置包数据403(即配置有效载荷块404和控制块406)来生成配置包。在调试设备处生成配置包。

[0140] 配置验证包412在服务器设备处生成。配置认证包412包括一组完整性指示符，诸如第一完整性指示符414、第二完整性指示符416。服务器从调试设备接收配置包402。配置包402包括配置有效载荷块404和控制块406。服务器通过基于配置有效载荷块404计算第一完整性指示符414以及基于控制块406计算第二完整性指示符416来生成配置块419，并且将第一完整性指示符414和第二完整性指示符416包括在配置块419中。服务器设备使用配置私有秘钥对配置验证包412进行签名。配置验证包412包括第一数字签名418。

[0141] 图5示意性示出根据本公开的示例性配置认证包502。配置认证包502由服务器设备生成。配置认证包502包括配置认证材料504。配置认证材料504包括验配师证书506，其可以使用证书密钥进行加密，所述证书密钥包括在由服务器设备使用包括在从调试设备接收的访问请求中的验配师标识符检索的验配师证书中。服务器使用存储在服务器设备中并用于配置目的的配置私有密钥，经由配置认证材料504获取第二数字签名508。配置认证包502包括第二数字签名508。

[0142] 图6示意性示出根据本公开在调试设备2、服务器设备4、附属设备10和听力设备8之间的示例性信令图示600。调试设备2可以被配置为将访问请求601发送到服务器设备4以及从服务器设备接收访问响应602。访问请求可以包括识别调试设备2的用户的验配师标识符。调试设备2将配置发起请求604发送到服务器设备4。配置发起请求604包括会话密钥、听力设备标识符，可选地听力设备数据的一部分(例如共享索引)，以及可选地会话计数器。服务器设备4用配置发起响应606进行响应，配置发起响应606包括配置密钥材料。调试设备2基于接收到的配置密钥材料和验配师在调试设备2上设计的配置数据来生成配置包。调试设备2将配置包608传输到服务器设备4。

[0143] 如步骤SS206、S207、S2071和S208所公开，服务器设备4生成配置验证包610。服务器设备4经由通信链路21或可选地经由调试设备2以及通信链路22和23将配置验证包610发送到附属设备10或安装在其上的用户应用。如步骤S203、S203a-c、S2081和S209所公开，服务器设备4生成配置认证包612。服务器设备4将配置认证包612发送到附属设备10或其上安装的用户应用。服务器设备4使用在服务器设备4和调试设备2之间共享的会话密钥来解密从调试设备2接收的配置包装608。服务器设备将消息614中所得的配置包发送到附属设备10或安装在其上的用户应用。然后，附属设备10可以将消息616中的配置认证包和消息618中的配置包传递给听力设备，从而可以进行安全的远程配置。

[0144] 图7示意性示出根据本公开的示例性调试设备2。调试设备2包括处理单元302、存储器单元301和接口303。调试设备2或处理单元302被配置为执行根据本公开的方法(诸如图2的方法100)的步骤中的任一个。处理单元302被配置为获取听力设备数据。处理单元302被配置为生成会话密钥，例如，作为随机数或伪随机数。处理单元302被配置为基于会话密

钥和听力设备标识符生成配置发起请求。接口303被配置为将配置发起请求传输到服务器设备。配置发起请求包括会话密钥、听力设备标识符，可选地听力设备数据的一部分(例如，共享索引)，以及可选地会话计数器。在传输前通过处理单元302使用配置发起公共秘钥加密配置发起请求。

[0145] 接口303被配置为从服务器设备接收配置发起响应，所述配置发起响应包括配置密钥材料。处理单元302被配置为例如使用会话密钥解密配置密钥材料。配置密钥材料可以包括配置密钥(诸如对称的)，以及可能地包括配置密钥计数器。

[0146] 处理单元302被配置为基于听力设备的配置数据并基于配置密钥材料生成配置包。配置包包括配置包数据。配置数据可以包括与听力设备相关的数据。与听力设备相关的数据可以包括听力设备设置和/或调试参数。

[0147] 处理单元302可以被配置为通过基于配置数据计算配置数据完整性指示符来生成配置包。处理单元302被配置为通过使用配置密钥材料加密配置数据和/或配置数据完整性指示符来生成配置包。配置包数据可以基于加密的配置数据和/或加密的配置数据完整性指示符。例如，配置包数据可以包括加密的配置数据和/或加密的配置数据完整性指示符。处理单元302可以被配置为通过例如使用会话秘钥加密配置包数据来生成配置包。

[0148] 接口303被配置为将配置包传输到服务器设备。处理单元302可以被配置为在传输配置包之后删除会话密钥和配置密钥材料。

[0149] 接口303被配置为将访问请求发送到服务器设备，并从服务器设备接收访问响应。

[0150] 接口303可以被配置为使用例如键盘和/或显示器与调试设备的用户(例如，验配师)进行通信。

[0151] 调试设备2或处理单元302被布置成执行如本文所公开的用于远程配置听力设备的方法。调试设备2或处理单元302可进一步包括多个可选功能模块，诸如被配置为执行步骤S101和S102的获取模块302a以及被配置为执行步骤S103和S106的生成模块302b中的任一个。获取模块302a可选地被配置为执行步骤S101a。生成模块302b可选地被配置为执行步骤S103a。生成模块302b可选地被配置为执行步骤S106a、S106b、S106c。处理单元302可进一步包括被配置为执行步骤S108的删除模块302c。每个功能模块302a-c的功能在上下文中被公开，其中功能模块302a-c可以在图2和随附文本中使用。一般来说，每个功能模块302a-c可以以硬件或软件来实现。优选地，功能模块302a-c中的一个或多个或全部功能模块302a-c可以由处理模块302实现，可能地与功能单元301和303协作。因此，处理模块302可被布置为从存储器模块301获取指令，如功能模块302a-c提供，并被布置为执行这些指令，从而执行如图2中公开的方法100的任何步骤。

[0152] 图8示意性出根据本公开的示例性服务器设备4。服务器设备4包括处理单元802、存储器单元801和接口803。存储器单元801可以包括可移除和不可移除数据存储单元，包括但不限于只读存储器(ROM)、随机存取存储器(RAM)等等。服务器设备4被配置为执行根据本公开的方法(诸如图3的方法200)的步骤中的任一个。

[0153] 服务器设备4或接口803被配置为从调试设备接收配置发起请求，所述配置发起请求包括听力设备标识符和会话密钥。

[0154] 服务器设备4或处理单元802被配置为基于会话密钥生成配置密钥材料。服务器设备4或处理单元802被配置为生成配置认证材料。服务器设备4或接口803被配置为将配置发

起响应传输到调试设备，所述配置发起响应包括配置密钥材料。服务器设备4或接口803被配置为从调试设备接收配置包，所述配置包包括配置有效载荷块和控制块。服务器设备4或处理单元802被配置为基于配置有效载荷块和控制块来计算完整性指示符集。服务器设备4或处理单元802被配置为基于完整性指示符集的至少一部分来生成配置块。服务器设备4或处理单元802可以被配置为经由配置块获取第一数字签名。服务器设备4或处理单元802被配置为基于配置块并可选地基于第一数字签名生成配置验证包。服务器设备4或处理单元802可以被配置为经由配置认证材料获取第二数字签名。服务器设备4或处理单元802被配置为基于配置认证材料并可选地基于第二签名生成配置认证包。服务器设备4或接口803被配置为将配置包、配置验证包和配置认证包传输到例如听力设备和/或附属设备。

[0155] 服务器设备4可以包括安全模块804，以用于执行诸如加密、解密和数字签名的加密功能。安全模块804可被实现为硬件安全模块，其与服务器设备4并置或远程定位。

[0156] 服务器设备4或处理单元802被布置为执行如本文所公开的用于支持听力设备的远程配置的方法。服务器设备4或处理单元802可进一步包括多个可选功能模块，诸如被配置为执行步骤S202、S203、S207、S208和S209的生成模块802a中的任一个。生成模块802a可选地被配置为执行步骤S203a-d。生成模块802a可选地被配置为执行步骤S202a。处理单元802可进一步包括被配置为执行步骤S2071和可选地执行S2081的获取模块802b。每个功能模块802a-b的功能在上下文中被公开，其中功能模块802a-b可在图3和随附文本中使用。一般来说，每个功能模块802a-b可以以硬件或软件来实现。优选地，功能模块802a-b中的一个或多个或者所有功能模块802a-b可以由处理模块802实现，可能地与功能单元801和803以及可选地与单元804协作。因此，处理模块802可被布置为从存储器模块801获取指令，如功能模块802a-b提供，并被布置为执行这些指令，从而执行如本文图3中公开的方法200的任何步骤。

[0157] 接口803可以被配置为使用例如键盘和/或显示器与服务器设备的用户进行通信。

[0158] 使用术语“第一”、“第二”、“第三”和“第四”等并不意味着特定的顺序，而是被包括以识别各个元素。此外，术语第一、第二等的使用不表示任何顺序或重要性，而是使用术语第一、第二等来区分一个元件与另一个元件。注意，词语第一和第二在这里和其他地方仅用于标记目的，并不意图表示任何特定的空间或时间排序。此外，第一元件的标记并不意味着存在第二元件，反之亦然。

[0159] 虽然已经示出和描述了特定的特征，但是应当理解，它们并不旨在限制所要求保护的发明，并且对于本领域技术人员来说将会显而易见的是，在不脱离所要求保护的发明的精神和范围的情况下，可作出各种改变和修改。因此，说明书和附图被认为是说明性的而不是限制性的意义。所要求保护的发明旨在涵盖所有替代方案、修改和等效物。

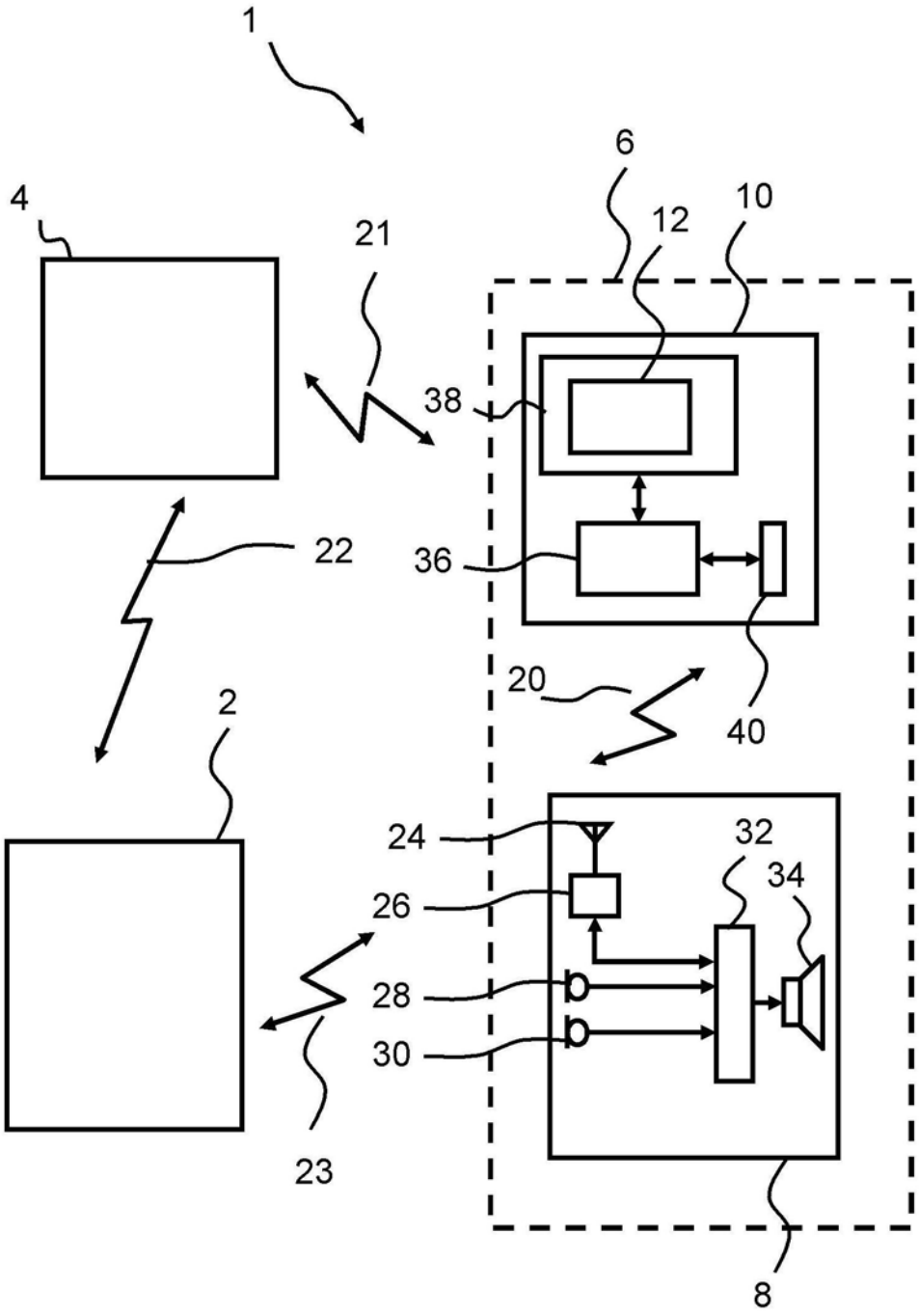


图1

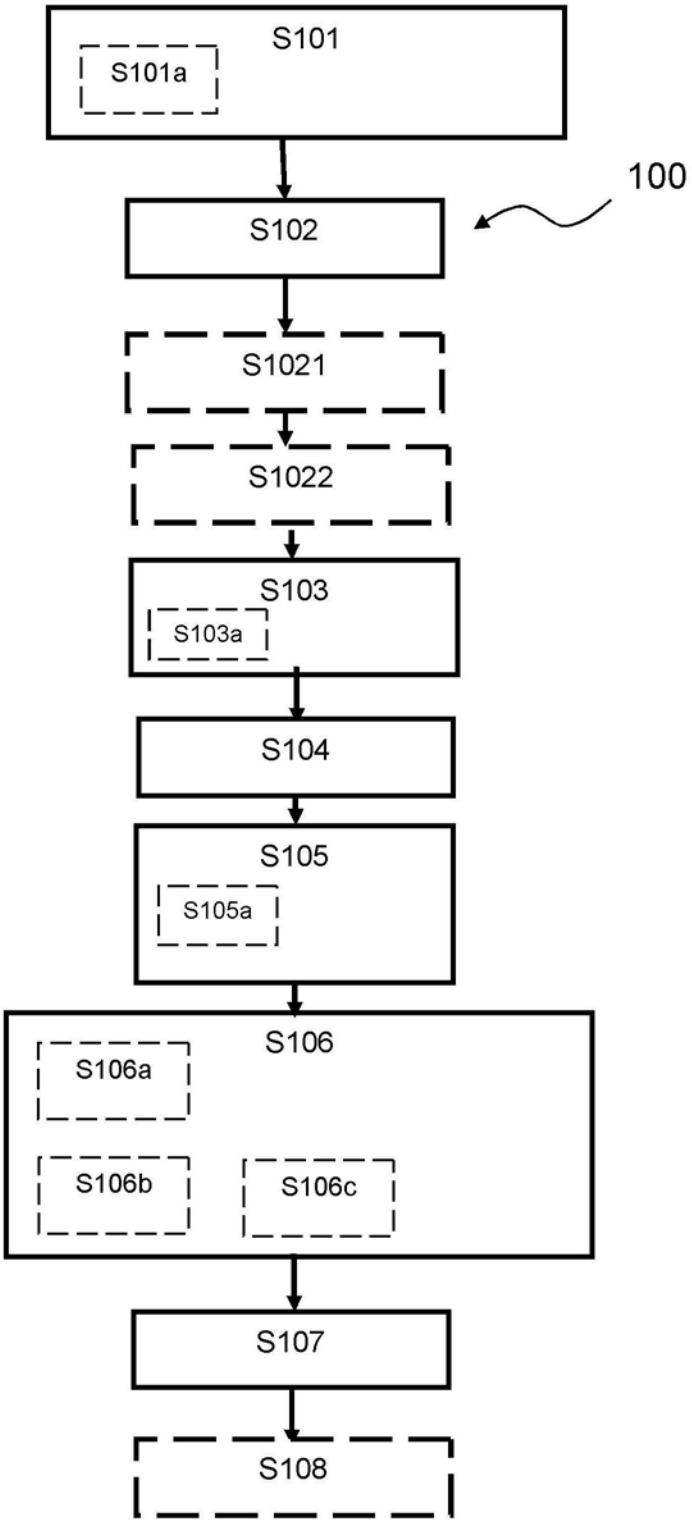

S101
S101a
100
S102
S1021
S1022
S103
S103a
S104
S105
S105a
S106
S106a
S106b
S106c
S107
S108

图2

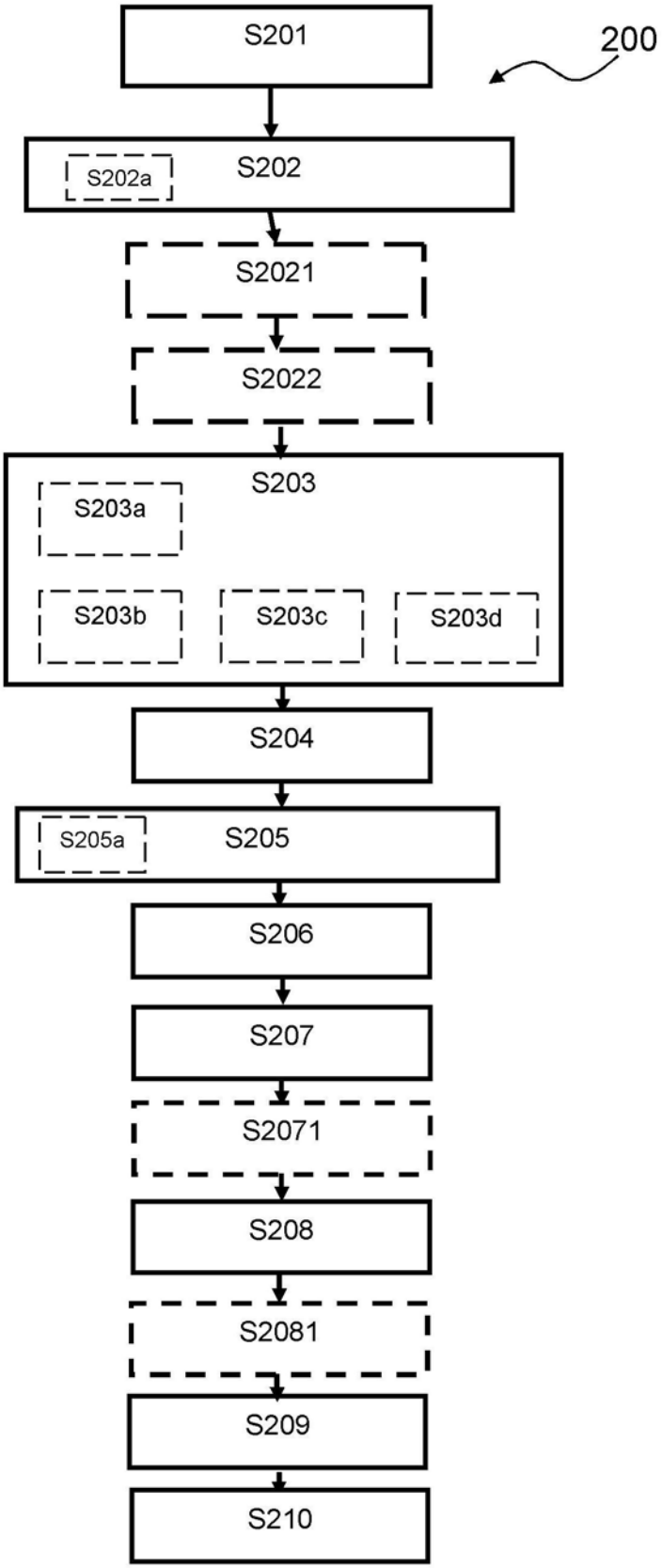

S201
200
S202
S202a
S2021
S2022
S203
S203a
S203b
S203c
S203d
S204
S205
S205a
S206
S207
S2071
S208
S2081
S209
S210

图3

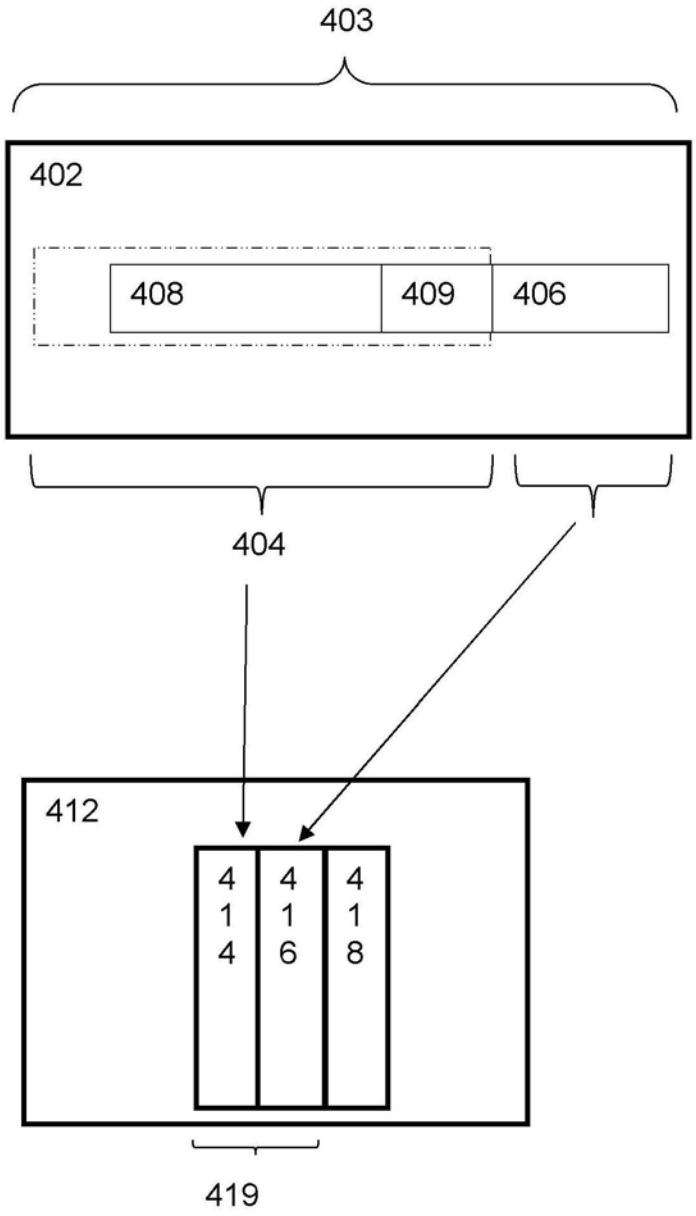


图4

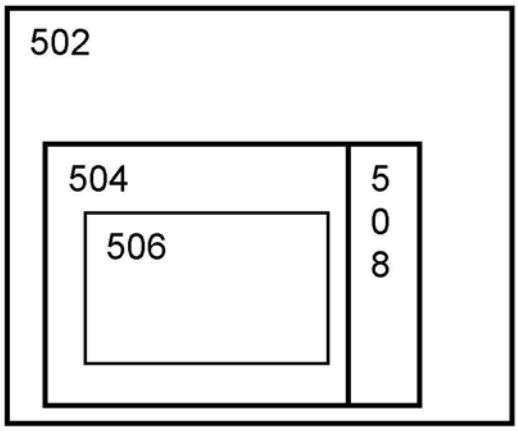


图5

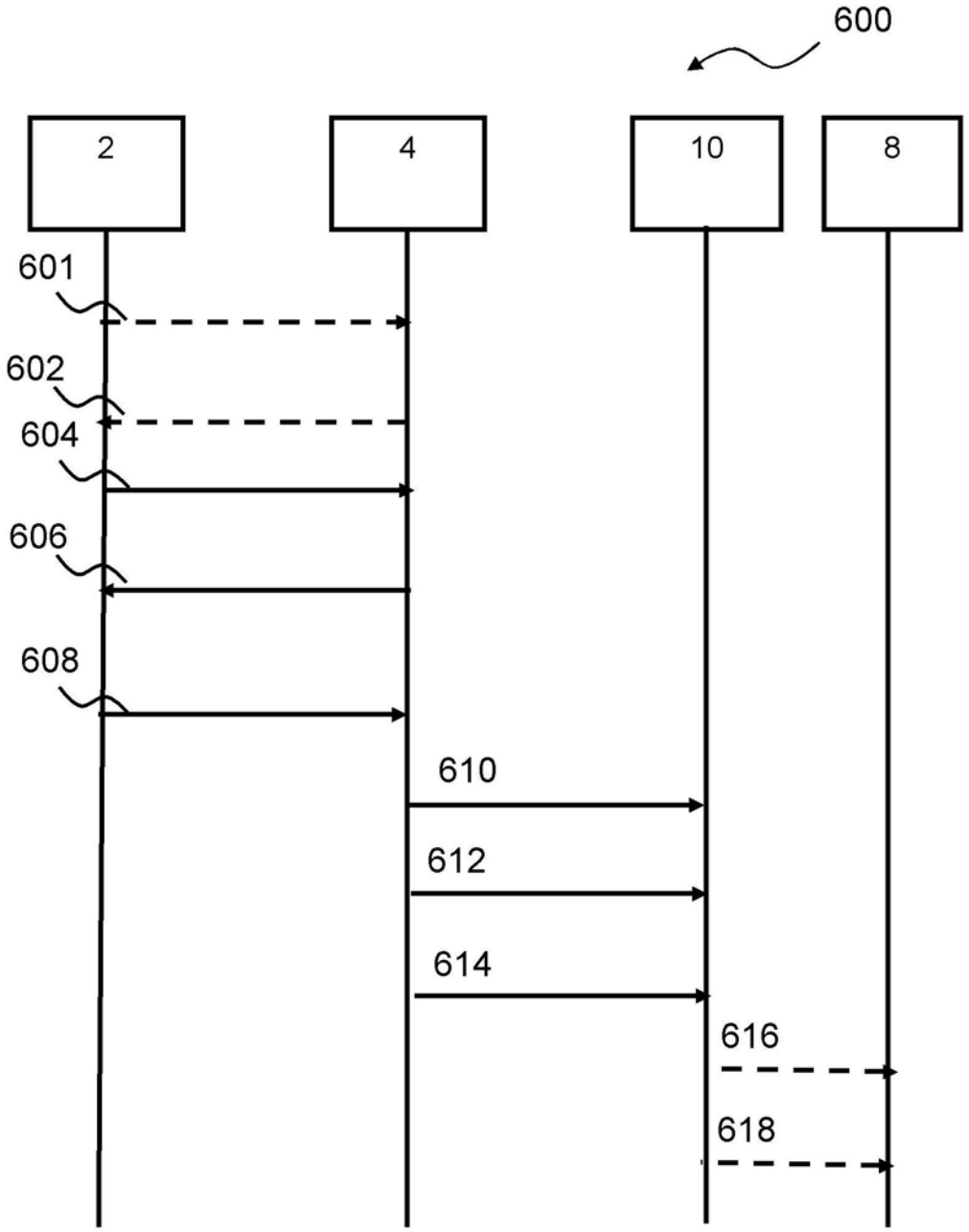


图6

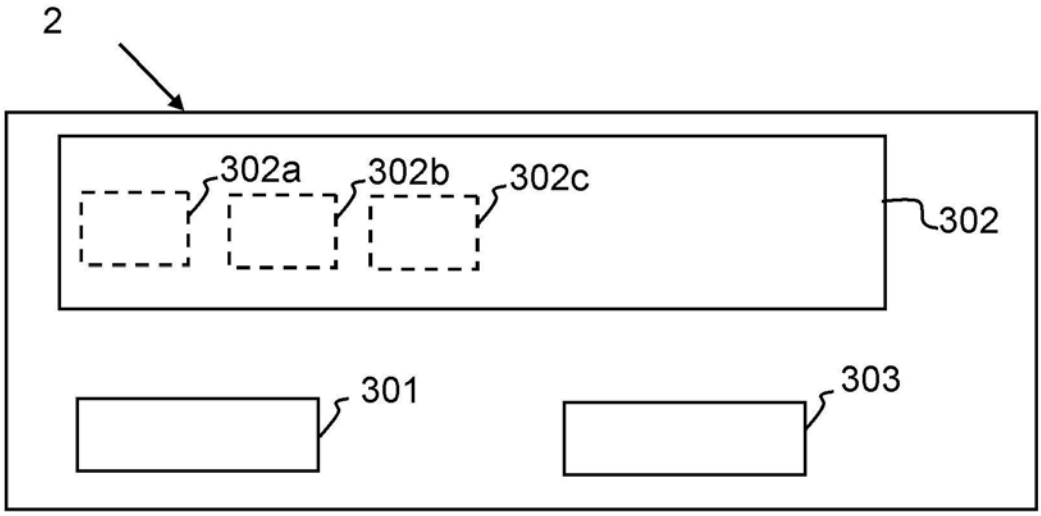


图7

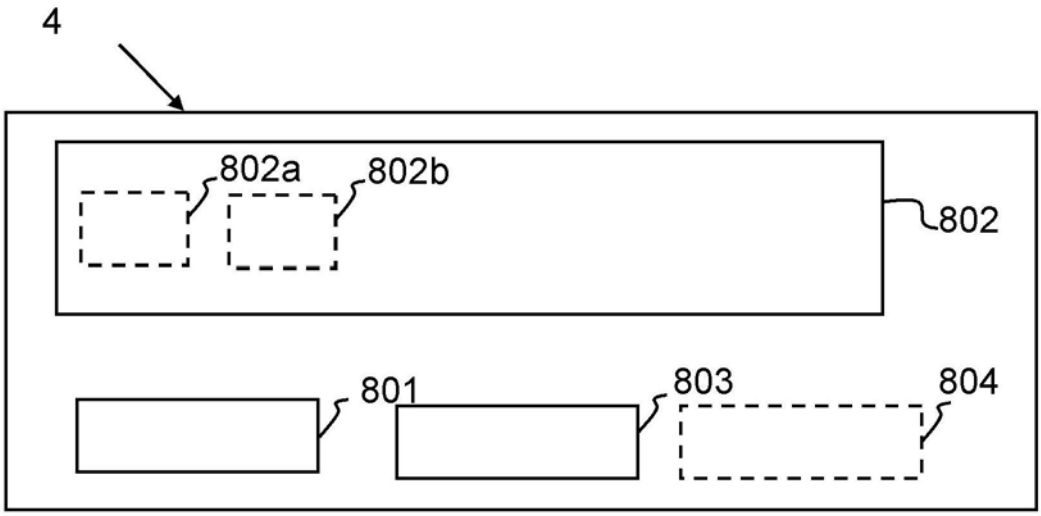


图8