



(10) 授权公告号 CN 114008967 B

(45) 授权公告日 2024.10.18

(21) 申请号 202080044558.3

(22) 申请日 2020.06.11

(65) 同一申请的已公布的文献号
申请公布号 CN 114008967 A

(43) 申请公布日 2022.02.01

(30) 优先权数据
19181035.7 2019.06.18 EP(85) PCT国际申请进入国家阶段日
2021.12.17(86) PCT国际申请的申请数据
PCT/EP2020/066179 2020.06.11(87) PCT国际申请的公布数据
W02020/254177 EN 2020.12.24

(73) 专利权人 皇家飞利浦有限公司

地址 荷兰艾恩德霍芬

(72) 发明人 O·加西亚莫尔琼
L·M·G·M·托尔胡伊泽恩
S·巴塔查里亚(74) 专利代理机构 永新专利商标代理有限公司
72002

专利代理师 刘兆君

(51) Int.Cl.
H04L 9/08 (2006.01)(56) 对比文件
CN 103326852 A, 2013.09.25
CN 106464490 A, 2017.02.22

审查员 曹彦

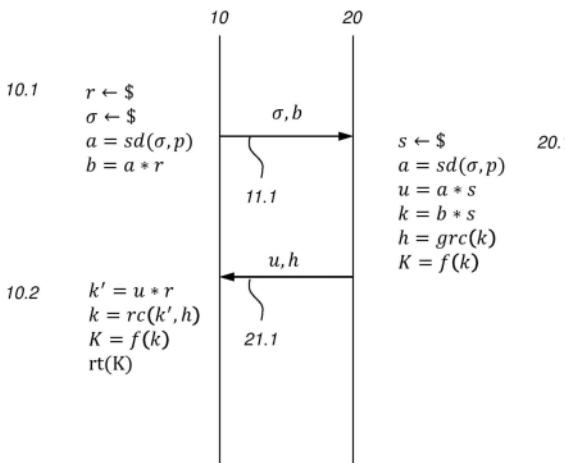
权利要求书6页 说明书23页 附图7页

(54) 发明名称

用于经认证的基于晶格的密钥协商或密钥
封装的方法和装置

(57) 摘要

一些实施例涉及具有第一密码设备(10)和第二密码设备(20)的系统。所述设备可以根据所述设备已知的预先共享秘密以及在它们之间交换的预先种子来计算最终种子。最终种子可用于导出公共对象(a)。



1. 一种用于与第一密码设备 (10) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的密码设备 (20), 所述密码设备 (20) 包括:

通信接口, 其被配置为使用所述基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议来与所述第一密码设备 (10) 通信,

处理器, 其被配置为:

根据以下来计算最终种子:

从所述第一密码设备 (10) 接收的预先种子,

预先共享秘密, 所述秘密在所述密码设备 (20) 与所述第一密码设备 (10) 之间预先共享, 以及

进一步的信息, 所述进一步的信息包括以下中的至少一个:

所述第一密码设备 (10) 和/或所述密码设备 (20) 的网络地址,

网络端口地址,

一天中的时间, 以及

交互计数器, 所述交互计数器由所述密码设备 (20) 和所述第一密码设备 (10) 维护并且至少每当导出共享密钥时增加;

使用确定性随机位生成器 (DRBG) 或伪随机数生成器 (PRNG) 来根据所述最终种子计算公共对象 (a);

获得与所述第一密码设备 (10) 相关联的第一公钥 (b), 并且获得与所述密码设备 (20) 相关联的第二私钥 (s), 所述第一公钥是在所述第一密码设备 (10) 处计算出的, 所述计算包括所述公共对象与所述第一密码设备 (10) 的第一私钥之间的乘法;

根据所述第二私钥 (s) 计算第二公钥 (u), 计算所述第二公钥 (u) 包括将所述第二私钥 (s) 与所述公共对象 (a) 相乘;

根据所述第一公钥 (b) 和所述第二私钥 (s) 计算第二原始共享密钥 (k*), 计算所述第二原始共享密钥 (k*) 包括所述第二私钥 (s) 与所述第一公钥 (b) 之间的乘法;

将所述第二公钥 (u) 传送到所述第一密码设备 (10)。

2. 根据权利要求1所述的用于与第一密码设备 (10) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的密码设备 (20), 其中, 所述预先共享秘密包括预先共享秘密。

3. 根据权利要求1所述的用于与第一密码设备 (10) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的密码设备 (20), 其中, 所述预先种子是以明文格式发送和接收的。

4. 根据权利要求1所述的用于与第一密码设备 (10) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的密码设备 (20), 其中, 所述预先种子是通过所述通信接口发送和接收, 但是所述预先共享秘密不通过所述通信接口发送和接收。

5. 根据权利要求1所述的用于与第一密码设备 (10) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的密码设备 (20), 其中, 所述最终种子还根据来自所述密码设备 (20) 与所述第一密码设备 (10) 之间的网络连接的配置数据计算。

6. 根据权利要求1所述的用于与第一密码设备 (10) 一起执行基于晶格的密钥交换KEX

或基于晶格的密钥封装KEM密钥协商协议的第二密码设备(20),其中,

所述第二密码设备(20)的所述处理器被配置为:

生成传输密钥(K),

通过应用封装函数,利用所述第二原始共享密钥(k^*)的至少部分来封装所述传输密钥(K),获得封装数据(c),

将所述封装数据(c)传送到所述第一密码设备(10),并且

所述第一密码设备(10)的所述处理器被配置为:

从所述第二密码设备(20)接收封装数据(c),

使用第一原始共享密钥(k')的至少部分对所述封装数据(c)解封装以获得传输密钥。

7.根据权利要求1所述的用于与第一密码设备(10)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第二密码设备(20),其中

所述第二密码设备(20)的所述处理器被配置为:

针对所述第二原始共享密钥(k^*)的系数中的至少部分来生成调和数据(h),所述调和数据包括允许减少在所述第一密码设备(10)和所述第二密码设备(20)处导出的第一原始密钥与第二原始密钥之间的差异的信息,

根据所述第二原始共享密钥(k^*)来生成传输密钥(K),

将所述调和数据(h)传送到所述第一密码设备(10),并且

所述第一密码设备(10)的所述处理器被配置为:

从所述第二密码设备(20)接收调和数据(h),

将调和函数中的所述调和数据(h)应用于第一原始共享密钥(k')的所述系数中的至少部分,

根据经调和的第一原始共享密钥(k')来生成传输密钥(K)。

8.根据权利要求1所述的用于与第一密码设备(10)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第二密码设备(20),其中,在计算所述第一公钥(b)和所述第二公钥(u)时与所述公共对象(a)相乘是噪声乘法。

9.根据权利要求6或7所述的用于与第一密码设备(10)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第二密码设备(20),其中,

所述第二密码设备(20)的所述处理器被配置为利用所述传输密钥对消息(m)进行加密,并且将所加密的消息传送到所述第一密码设备(10),所述第一密码设备(10)的所述处理器被配置为利用所述传输密钥对所加密的消息进行解密,并且验证所述消息(m),和/或

所述第一密码设备(10)的所述处理器被配置为利用所述传输密钥对消息(m)进行加密,并将所加密的消息传送到所述第二密码设备(20),所述第二密码设备(20)的所述处理器被配置为利用所述传输密钥对所加密的消息进行解密,并且验证所述消息(m)。

10.根据权利要求6或7所述的用于与第一密码设备(10)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第二密码设备(20),其中,所述传输密钥是随机的、和/或短暂的和/或对称的和/或独立于所述第一公钥(b)。

11.根据权利要求7所述的用于与第一密码设备(10)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第二密码设备(20),其中:

所述第一公钥和所述第二公钥、所述第一私钥和所述第二私钥、所述第一原始密钥和

所述第二原始密钥以及所述公共对象是有限域或环上的矩阵,

所述第一公钥和所述第二公钥、所述第一私钥和所述第二私钥、所述第一原始密钥和所述第二原始密钥以及所述公共对象是有限域或环上的多项式。

12. 根据权利要求6或7所述的用于与第一密码设备(10)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第二密码设备(20), 其中, 网络配置数据是利用所述传输密钥加密发送的。

13. 一种用于与第二密码设备(20)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备(10), 所述第一密码设备(10)包括:

通信接口, 其被配置为使用所述基于晶格的密钥交换KEX或所述基于晶格的密钥封装KEM密钥协商协议与所述第二密码设备(20)通信,

处理器, 其被配置为:

选择预先种子并将所述预先种子发送到所述第二密码设备(20);

根据以下来计算最终种子:

所述预先种子,

预先共享秘密, 所述秘密在所述第二密码设备(20)和所述第一密码设备(10)之间预先共享, 以及

进一步的信息, 所述进一步的信息包括以下中的至少一个:

所述第一密码设备(10)和/或所述第二密码设备(20)的网络地址,

网络端口地址,

一天中的时间, 以及

交互计数器, 所述交互计数器由所述第二密码设备(20)和所述第一密码设备(10)维护并且至少每当导出共享密钥时增加;

使用确定性随机位生成器(DRBG)或伪随机数生成器(PRNG)来根据所述最终种子计算公共对象(a);

获得与所述第一密码设备(10)相关联的第一私钥(r)并根据所述第一私钥(r)来计算第一公钥(b), 计算所述第一公钥(b)包括将所述第一私钥(r)与所述公共对象(a)相乘, 并且将所述第一公钥(b)传送到所述第二密码设备(20);

从所述第二密码设备(20)接收第二公钥(u);

根据所述第二公钥(u)和所述第一私钥(r)计算第一原始共享密钥(k'), 计算所述第一原始共享密钥(k')包括所述第二公钥(u)与所述第一私钥(r)之间的乘法。

14. 根据权利要求13所述的用于与第二密码设备(20)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备(10), 其中, 所述预先共享秘密包括预先共享密码。

15. 根据权利要求13所述的用于与第二密码设备(20)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备(10), 其中, 所述预先种子是以明文格式发送和接收的。

16. 根据权利要求13所述的用于与第二密码设备(20)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备(10), 其中, 所述预先种子是通过所述通信接口发送和接收, 但是所述预先共享秘密不通过所述通信接口发送和接收。

17. 根据权利要求13所述的用于与第二密码设备(20)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备(10), 其中, 所述最终种子还根据来自所述第二密码设备(20)与所述第一密码设备(10)之间的网络连接的网络配置数据计算。

18. 根据权利要求13所述的用于与第二密码设备(20)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备(10), 其中,

所述第二密码设备(20)的所述处理器被配置为:

生成传输密钥(K),

通过应用封装函数, 利用第二原始共享密钥(k^*)的至少部分来封装所述传输密钥(K), 获得封装数据(c),

将所述封装数据(c)传送到所述第一密码设备(10), 并且

所述第一密码设备(10)的所述处理器被配置为:

从所述第二密码设备(20)接收封装数据(c),

使用所述第一原始共享密钥(k')的至少部分对所述封装数据(c)解封装以获得传输密钥。

19. 根据权利要求13所述的用于与第二密码设备(20)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备(10), 其中

所述第二密码设备(20)的所述处理器被配置为:

针对第二原始共享密钥(k^*)的系数中的至少部分来生成调和数据(h), 所述调和数据包括允许减少在所述第一密码设备(10)和所述第二密码设备(20)处导出的第一原始密钥与第二原始密钥之间的差异的信息,

根据所述第二原始共享密钥(k^*)来生成传输密钥(K),

将所述调和数据(h)传送到所述第一密码设备(10), 并且

所述第一密码设备(10)的所述处理器被配置为:

从所述第二密码设备(20)接收调和数据(h),

将调和函数中的所述调和数据(h)应用于所述第一原始共享密钥(k')的所述系数中的至少部分,

根据经调和的第一原始共享密钥(k')来生成传输密钥(K)。

20. 根据权利要求13所述的用于与第二密码设备(20)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备(10), 其中, 在计算所述第一公钥(b)和所述第二公钥(u)时与所述公共对象(a)相乘是噪声乘法。

21. 根据权利要求18或19所述的用于与第二密码设备(20)一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备(10), 其中,

所述第二密码设备(20)的所述处理器被配置为利用所述传输密钥对消息(m)进行加密, 并且将所加密的消息传送到所述第一密码设备(10), 所述第一密码设备(10)的所述处理器被配置为利用所述传输密钥对所加密的消息进行解密, 并且验证所述消息(m), 和/或

所述第一密码设备(10)的所述处理器被配置为利用所述传输密钥对消息(m)进行加密, 并将所加密的消息传送到所述第二密码设备(20), 所述第二密码设备(20)的所述处理器被配置为利用所述传输密钥对所加密的消息进行解密, 并且验证所述消息(m)。

22. 根据权利要求18或19所述的用于与第二密码设备 (20) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备 (10), 其中, 所述传输密钥是随机的、和/或短暂的和/或对称的和/或独立于所述第一公钥 (b)。

23. 根据权利要求19所述的用于与第二密码设备 (20) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备 (10), 其中:

所述第一公钥和所述第二公钥、所述第一私钥和第二私钥、所述第一原始密钥和所述第二原始密钥以及所述公共对象是有限域或环上的矩阵,

所述第一公钥和所述第二公钥、所述第一私钥和所述第二私钥、所述第一原始密钥和所述第二原始密钥以及所述公共对象是有限域或环上的多项式。

24. 根据权利要求18或19所述的用于与第二密码设备 (20) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的第一密码设备 (10), 其中, 网络配置数据是利用所述传输密钥加密发送的。

25. 一种用于与第一密码设备 (10) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的密码方法 (400), 所述方法包括:

根据以下来计算 (410) 最终种子:

从所述第一密码设备 (10) 接收的预先种子,

预先共享秘密, 所述秘密在第二密码设备 (20) 与所述第一密码设备 (10) 之间预先共享, 以及

进一步的信息, 所述进一步的信息包括以下中的至少一个:

所述第一密码设备 (10) 和/或所述第二密码设备 (20) 的网络地址,

网络端口地址,

一天中的时间, 以及

交互计数器, 所述交互计数器由所述第二密码设备 (20) 和所述第一密码设备 (10) 维护并且至少每当导出共享密钥时增加;

使用确定性随机位生成器 (DRBG) 或伪随机数生成器 (PRNG) 来根据所述最终种子计算 (415) 公共对象 (a);

获得 (420) 与所述第一密码设备 (10) 相关联的第一公钥 (b), 并且获得与所述第二密码设备 (20) 相关联的第二私钥 (s), 所述第一公钥是在所述第一密码设备 (10) 处计算出的, 所述计算包括在所述公共对象与所述第一密码设备 (10) 的第一私钥之间的乘法;

根据所述第二私钥 (s) 计算 (425) 第二公钥 (u), 计算所述第二公钥 (u) 包括将所述第二私钥 (s) 与所述公共对象 (a) 相乘;

根据所述第一公钥 (b) 和所述第二私钥 (s) 计算 (430) 第二原始共享密钥 (k*), 计算所述第二原始共享密钥 (k*) 包括所述第二私钥 (s) 与所述第一公钥 (b) 之间的乘法;

将所述第二公钥 (u) 传送 (435) 到所述第一密码设备 (10)。

26. 一种用于与第二密码设备 (20) 一起执行基于晶格的密钥交换KEX或基于晶格的密钥封装KEM密钥协商协议的密码方法 (450), 所述方法包括:

选择 (460) 预先种子并将所述预先种子发送到所述第二密码设备 (20);

根据以下来计算 (465) 最终种子:

所述预先种子,

预先共享秘密,所述秘密在所述第二密码设备(20)和第一密码设备(10)之间预先共享,以及

进一步的信息,所述进一步的信息包括以下中的至少一个:

所述第一密码设备(10)和/或所述第二密码设备(20)的网络地址,

网络端口地址,

一天中的时间,以及

交互计数器,所述交互计数器由所述第二密码设备(20)和所述第一密码设备(10)维护并且至少每当导出共享密钥时增加;

使用确定性随机位生成器(DRBG)或伪随机数生成器(PRNG)来根据所述最终种子计算(470)公共对象(a);

获得(475)与所述第一密码设备(10)相关联的第一私钥(r)并根据所述第一私钥(r)来计算第一公钥(b),计算所述第一公钥(b)包括将所述第一私钥(r)与所述公共对象(a)相乘,并且将所述第一公钥(b)传送到所述第二密码设备(20);

从所述第二密码设备(20)接收(480)第二公钥(u);

根据所述第二公钥(u)和所述第一私钥(r)来计算(485)第一原始共享密钥(k'),计算所述第一原始共享密钥(k')包括所述第二公钥(u)与所述第一私钥(r)之间的乘法。

27.一种瞬态或非瞬态计算机可读介质(1000),包括表示指令的数据(1020),所述指令在由处理器系统运行时使所述处理器系统执行根据权利要求25和/或26所述的方法。

用于经认证的基于晶格的密钥协商或密钥封装的方法和设备

技术领域

[0001] 当前公开的主题涉及第一密码设备、第二密码设备、第一密码方法、第二密码方法和计算机可读介质。

背景技术

[0002] 在密码学中,密钥协商协议是两方或多方可以就这样的密钥达成一致的协议。例如,商定的密钥可以用于保护各方之间的进一步通信,例如,认证和/或加密进一步的通信。窃听双方之间所有通信的攻击者应该对密钥一无所知。然而,虽然看到相同通信的攻击者一无所知或所知甚少,但双方自己可以推导出共享密钥。

[0003] 实用的密钥协商协议于1976年引入,当时Whitfield Diffie和Martin Hellman引入了公钥密码学的概念。他们提出了一种在两方之间密钥协商的系统,该系统利用了具有 q 个元素的有限域 $GF(q)$ 上计算对数的明显困难。使用该系统,两个用户可以就对称密钥达成一致。

[0004] 密钥协商协议在多方通信的许多应用中是有用的,例如,在诸如物联网、自组无线网络等应用领域中。密钥协商可用于保护设备之间的链接。另一示例是阅读器和电子标签(例如读卡器和智能卡)或标签阅读器和标签(例如RFID标签或NFC标签)之间的通信。

[0005] 为了促进各方之间的安全通信,密钥协商协议有时被进一步细分为密码密钥交换(KEX)和密码密钥封装(KEM)方案。密码密钥封装(KEM)方案使用非对称密码在两方之间建立共享秘密,使用各方的公开已知(例如,公钥)和秘密拥有(例如,秘密密钥)值。

[0006] KEX方案涉及每一方交换公钥,然后由另一方连同自己的秘密密钥单独使用以计算公共共享秘密。KEX方案的公知示例是上面提到的Diffie-Hellman密钥交换,其安全性基于解决离散对数问题。通常,双方都可以影响结果,因此任何一方都不能强制选择密钥。一些KEX方案的有趣特征在于,实际上最终的共享秘密永远不会在双方之间交换,甚至不以加密形式交换,而是由双方在每一端独立地计算。这导致了称为前向保密的期望特征,确保了即使未来攻击者损害一方的长期密钥也不会损害过去交换的加密消息的保密性。

[0007] KEM方案通过一方(通常是通信的发起者)使用非对称密码术在两个实体或双方之间建立共享秘密,以使用另一方的公钥进行加密并将共享秘密传输给所述另一方(称为响应者),所述另一方然后可以使用她的秘密密钥进行解密,并且然后使用它与发起方进行安全通信。KEM方案无法实现前向保密,因为任何损坏一方过去会话的密钥并记录该会话中各方之间交换的所有消息的攻击者都可以恢复该特定会话的共享秘密。

[0008] 自从Diffie和Hellman的论文发表以来,人们提出了新的担忧。由于物联网安全需求的增加,密钥交换方案还需要实现高效率和低通信或带宽要求。此外,密钥协商协议最好是安全的,可以抵御经典以及具有量子能力的对手。

[0009] 此外,这些密钥协商协议的缺点是它们不对各方进行认证。这使它们容易受到中间人(MITM)攻击。在中间人攻击中,攻击者可能将自己置于第一方和第二方之间。然后攻击者可以与第一方协商第一共享密钥并与第二方协商第二共享密钥。因此,攻击者能够解密

所有内容。通常,KEX和KEM类型的协议两者都需要例如数字签名来避免该问题。签名是在轻量级协议中通常也避免的操作。

[0010] 解决此的一种方法是所谓的经认证密钥交换(AKE)。AKE协议可以同时协商密钥和认证通信方的身份。一种特别重要的AKE是基于密码的AKE(PAKE)。PAKE利用在密码学上不安全的人类可记忆的密码(或密码短语),来认证和协商对称会话密钥。在PAKE中,密码可以由双方预先共享。

[0011] 在Xinwei Gao等人的论文“Efficient Implementation of Password-Based Authenticated Key Exchange from RLWE and Post-Quantum TLS”中,在此通过引用包括进来,在该论文的图2中提出了一种基于后量子密码的认证密钥交换(PAKE)协议,称为RLWE-PPK。

[0012] RLWE-PPK是在具有预先共享口令pwd的双方(i方和j方)之间的协议。每一方根据共享密码来计算出两个不同的散列: $\gamma_1 = H_1(\text{pwd})$ 和 $\gamma_2 = H_2(\text{pwd})$,其用于在传输给另一方之前和之后掩蔽(mask)和去掩蔽(unmask)各方的公钥。为了计算共享密钥,每一方都需要计算进一步的散列,使散列总数达到每方三个。RLWE-PPK是一种两轮隐式认证密钥协议。隐式认证意味着可以不计算对认证的明确确认,但是如果认证失败,则各方将无法获得相同的密钥,这继而可以保护通信不被泄露给未经认证的一方。

[0013] 已知的协议有几个缺点。例如,它要求为每个密钥协议计算三个散列。对于资源受限的设备,这是一种负担。此外,已知协议要求公钥保持机密,因为可以根据公钥和窃听通信的知识来计算密码散列。

发明内容

[0014] 具有改进的认证密钥协商的设备和/或方法将是有利的。密码设备和方法在本文中被阐述并且被要求保护旨在解决这些和其它问题。

[0015] 现有的密钥协商协议,即使是量子安全的,通常也没有经过隐式或显式的认证。如果现有的密钥协商协议可以扩展为经认证的密钥协商协议,那将是有利的。经认证的密钥协商协议更适合用于两方需要验证通信信道的真实世界场景中。

[0016] 当前公开的主题包括第一密码设备、第二密码设备、第一密码方法、第二密码方法和计算机可读介质。第一和第二密码设备可以被配置为根据预先共享秘密(例如密码)计算最终种子,并形成在设备之间交换的预先种子。最终种子可用于计算公共对象,公共对象又可用于计算公钥,例如以执行密钥协商协议。

[0017] 实施例有助于避免中间人攻击。由于第一密码设备(也称为第一方)和第二密码设备(也称为第二方)具有预先共享秘密,因此它们可以导出可以从中导出公钥的公共对象。攻击者无法访问密码,并且因此无法计算公共对象。因此,他不能将自己置于各方之间的通信中,因为执行正确计算需要公共对象。有趣的是,密码的强度主要与认证的强度有关;导出的共享密钥的强度可能不受影响。特别地,根据实施例的密钥协商协议可以与没有认证的情况一样强,例如抗量子。

[0018] 此外,可以有效地实施实施例。例如,在实施例中,各方可以计算少至单个散列函数,例如以计算最终种子。如果需要,则可以在没有非对称数字签名的情况下获得显式认证。此外,不要求公钥是秘密的。注意,根据实施例,所有或大多数基于NIST后量子密码术

(PQC) 晶格的候选可以适用于认证。

[0019] 在实施例中,预先种子可以通过通信信道以明文通信,而预先共享秘密不通过信道或不以明文传送。例如,通信信道还可以用于以密钥协商协议在设备之间交换的其它数据。

[0020] 当前公开的主题的各方面包括密码方法。

[0021] 方法的实施例可以作为计算机实现的方法实现于计算机上,或者在专用硬件中,或者在两者的组合中。用于方法的实施例的可执行代码可以存储在计算机程序产品上。计算机程序产品的示例包括存储器设备、光存储设备、集成电路、服务器、在线软件等。优选地,计算机程序产品包括存储在计算机可读介质上的非瞬态程序代码,用于当在计算机上运行所述程序产品时执行方法的实施例。

[0022] 在实施例中,计算机程序包括计算机程序代码,当计算机程序在计算机上运行时,所述计算机程序代码适于执行方法的实施例的所有或部分步骤。优选地,计算机程序体现在计算机可读介质上。

[0023] 当前公开的主题的另一方面提供了一种使计算机程序可用于下载的方法。当计算机程序被上传到例如Apple的App Store、Google的Play Store或Microsoft的Windows Store时,以及当计算机程序可从此类商店下载时,将使用该方面。

附图说明

[0024] 将参考附图通过示例的方式描述进一步的细节、方面和实施例。图中的元件是为了简单和清楚而示出的并且不一定按比例绘制。在图中,对应于已经描述的元件的元件可以具有相同的附图标记。在图中,

[0025] 图1示意性地示出了KEX协议的实施例的示例,

[0026] 图2示意性地示出了KEM协议的实施例的示例,

[0027] 图3示意性地示出了协议的实施例的示例,

[0028] 图4示意性地示出了根据实施例的密码系统的示例,

[0029] 图5a示意性地示出了根据实施例的密码方法的示例,

[0030] 图5b示意性地示出了根据实施例的密码方法的示例,

[0031] 图6a示意性地示出了根据实施例的具有包括计算机程序的可写部分的计算机可读介质,

[0032] 图6b示意性地示出了根据实施例的处理器系统的表示。

[0033] 附图标记列表:

[0034] 10 第一密码设备

[0035] 20 第二密码设备

[0036] 10.1-10.3 密码操作

[0037] 11.1 密码消息

[0038] 20.1-20.2 密码操作

[0039] 21.1、21.2 密码消息

[0040] 13 界外通信

[0041] 14-15 密钥协商协议

[0042]	16-17	消息
[0043]	31	登记阶段
[0044]	32	密钥协商阶段
[0045]	33	使用阶段
[0046]	300	第一密码设备
[0047]	301	密码系统
[0048]	305	通信接口
[0049]	315	公钥/私钥生成器
[0050]	325	原始密钥生成器
[0051]	335	调和单元
[0052]	340	解封装单元
[0053]	350	第二密码设备
[0054]	355	通信接口
[0055]	360	公钥获取器
[0056]	365	公钥/私钥生成器
[0057]	375	原始密钥生成器
[0058]	385	调和数据生成器
[0059]	390	封装器
[0060]	1000	计算机可读介质
[0061]	1010	可写部分
[0062]	1020	计算机程序
[0063]	1110	集成电路
[0064]	1120	处理单元
[0065]	1122	存储器
[0066]	1124	(一个或多个)专用集成电路
[0067]	1126	通信元件
[0068]	1130	互连
[0069]	1140	处理器系统

具体实施方式

[0070] 虽然当前公开的主题可以有多种不同形式的实施例,但在附图中示出并且将在本文中详细描述一个或多个具体实施例,应理解本公开将被视为本公开主题的原理的示例,并且不旨在将其限制于所示和描述的特定实施例。

[0071] 在下文中,为了理解起见,在操作中描述实施例的元件。然而,很明显,各个元件被布置为执行被描述为由它们执行的功能。

[0072] 此外,当前公开的主题不限于实施例,因为可以组合本文描述的或在互不相同的从属权利要求中记载的特征。

[0073] 下面公开了各种实施例。在图1-3中,描述了可以为其配置第一密码设备10和第二密码设备20的各种协议。特别地,第一密码设备10和第二密码设备20可以被布置用于密钥

协商协议,特别用于认证密钥协商协议,更特别地用于密码认证密钥协商协议,或密码认证密钥交换(PAKE)。

[0074] 实施例可以基于所谓的噪声乘法。例如,为了从私钥导出公钥,第一密码设备10和第二密码设备20可以被配置为将公共对象(a)与私钥相乘以获得使用噪声乘法的公钥。噪声乘法的许多示例是已知的,例如,在诸如Round5、Saber、Kyber、NewHope和Frodo等密码密钥协商协议中使用。这些是基于晶格的密钥交换和/或密钥封装机制的示例,它们允许双方就公共密钥达成一致。在那些方案中,参数a(其通常是公开的)可用于分别从设备10和设备20的秘密r和s获得公钥分量b和u。可以使用至少两种密钥协商变体:KEX协议和KEM协议。在图1-2中使用以下符号:

[0075] • a代表第一密码设备10和第二密码设备20已知的公共对象。例如,公共对象可以是例如给定环中的多项式,例如RLWE或RLWR中使用的环,或具有整数条目的矩阵,例如LWE或LWR中使用的矩阵,或具有多项式条目的矩阵,

[0076] • r和s代表各方(例如设备10和20)的秘密。

[0077] • b和u代表各方的公钥或公钥份额。例如,作为 $a*r$ 或 $a*s$ 的噪声乘积获得。 $*$ 操作可以代表噪声乘法。噪声乘法是底层密码问题的单向函数,例如(R) LWE或(R) LWR或它们的模块版本等。

[0078] 例如,当提到LWR $a*r$ 时,可以实现为 $\text{Round}((Ar \pmod{q}), p, q)$ 。这可以是乘积r,其为长度为n的向量乘以 $n \times n$ 方阵A模q。然后通过执行 $p/q(Ar \pmod{q})$ 将结果舍入为整数p和q,其中 $p < q$ 。

[0079] • c代表封装的数据

[0080] • h代表辅助数据,包括调和位

[0081] • 函数sd被配置为根据其输入来产生最终种子 τ ,并根据最终种子 τ 来生成公共对象a。

[0082] • 函数grc是针对其输入生成调和数据的函数。例如,函数grc(k)可以被配置为从原始密钥k返回调和位。函数grc也可以称为get_reconciliation(k)。

[0083] • 函数rc是使用调和数据调和原始密钥的函数。例如,rc(k', h)可以是在给定调和位h的情况下调和原始密钥k的函数。函数rc也可以称为reconciliate(k', h)。

[0084] • 函数ecp是使用原始密钥封装数据的函数。例如,ecp(k, K)可以表示传输密钥K是用原始密钥k封装的。例如,封装函数可以使用密钥k掩蔽密钥K,使得k中的错误对m的影响有限,例如线性影响。例如,如果k是 Z_q 上的元素,例如向量、矩阵或多项式,则密钥K也可以在 Z_q 中表示。

[0085] 封装可以逐分量进行,例如, $c = k + K \cdot (q/2) \pmod{q}$ 。模数q可以是偶数,并且特别地可以是2的幂。传输密钥K是可以用作密钥协商协议的结果的密钥。例如,传输密钥可用于保护各方之间的进一步消息。进一步的保护可以是进一步消息的认证和/或加密。

[0086] 函数dcp是对封装数据进行解封装的函数,例如dcp(c, k')可以使用原始密钥k'对数据c进行解封装并返回例如位串K。函数dcp也可以被称为decapsulate(c, k')。例如,为解封装可以减去k'并舍入到q/2的最接近倍数。

[0087] 在实施例中,特定于各方的附加信息用于导出最终种子 τ ,该信息被称为上下文信息。上下文信息可以包括秘密信息p,例如,针对不信任方的秘密,例如除了第一密码设备10

和第二密码设备20之外的各方,或者除了第一密码设备10和第二密码设备20以及多个信任方(例如制造商)之外的各方。上下文信息可以是非秘密的,例如公开的。使用上下文信息来推导最终种子可以提高对其通信信道的真实性和新鲜度的保证。在密钥协商协议中共享的非秘密信息(例如,预先种子 σ)与虽非秘密但在密钥协商协议本身中未共享的其它信息 z 之间进行了区分。其它信息 z 的示例包括网络配置数据、公共随机信标等。

[0088] 例如,为了获得密码认证密钥交换(PAKE),各方可以共享秘密 p ,例如密码,例如PIN。各方可以将针对他们的通信链路的参数 a 计算为 $a = \text{drbg}(\text{hash}(\sigma, p))$,其中 σ 是预先种子,也称为公共种子,例如可以在协议期间甚至以明文交换的种子。预先种子可用作输入以从中导出最终种子 τ 。公共对象可以从最终种子 τ 导出。

[0089] 通过这种构造,如果各方共享相同的 p (其至少是隐式认证的),则他们将建立安全连接。交换的公共分量 b 和 u 不提供有关 p 的信息,因为 s 和 r 也是秘密。特别地,如果 s 和 r 是随机选择的,则可以高度保证 b 和 u 不提供有关 p 的信息。注意,链接的安全性不依赖于 p 中熵的量,例如在PIN中,因为密钥 K 中的机密性保证不依赖于公共对象的保密性。这种方法的优点包括:(i)获得PAKE需要计算的散列更少,以及(ii)更容易集成到现有的NIST PQC提议中,所述提议从种子计算公共对象 a ,例如 $a = \text{drbg}(\text{seed})$ 。集成可以包括改变获得种子的方式。

[0090] 例如,在实施例中,各方被配置为:

[0091] -获得公共的预先种子 σ 。例如,第一方可以生成预先种子,例如通过使用随机数生成器来生成其。第一方可以将预先种子发送给第二方。从这个意义上,预先种子可以被视为公共的,因为它可以在没有密码保护的情况下共享。

[0092] -获得依赖于上下文的输入,例如秘密 p ,例如密码,和/或其它信息 z ,根据其可以计算最终种子 τ ,例如, $\tau = \text{Hash}(\sigma | p)$,例如, $\tau = \text{Hash}(\sigma | p | z)$ 等,其中 $\text{hash}()$ 表示散列函数, $|$ 表示串联。最终种子 τ 被用于获得在双方中的每一方处的公共对象 a 。例如,依赖于上下文的公共对象例如可以通过应用 drbg 来应用,例如,确定性随机位生成器,或PRNG等,

[0093] 例如, $a = \text{drbg}(\tau)$ 。

[0094] 有趣的是,可以使用依赖于上下文的公共对象,例如,特定于当前密钥协商。这可用于提供隐式认证,例如,当使用预先共享秘密时。这可用于增加对中间人攻击的抵抗。这可用于增加对公共对象的预计算攻击的抵抗。

[0095] 在许多不同的领域或环中都知道许多噪声乘法。例如,可以通过执行真正的乘法并添加噪声源来实现噪声乘法。例如,噪声可以是例如从噪声源生成的显式噪声,或例如通过对结果进行舍入得到的隐式噪声。例如,为了对模 q 乘法进行舍入,人们可以从 $\text{mod } q$ 元素缩放到 $\text{mod } p$ 元素,其中 $p < q$,例如,乘以 p/q 并对结果进行舍入。对结果进行舍入的各种选择是可能的,例如,向下、向上舍入到最近的整数,舍入可以包括添加值,例如以减少偏差等。噪声源还可以或替代地包括向乘法结果添加显式噪声,例如高斯噪声。

[0096] 例如,第一和第二公钥、第一和第二私钥、第一和第二原始密钥以及公共对象可以是有限域或环上的矩阵或向量。例如,第一和第二公钥、第一和第二私钥、第一和第二原始密钥以及公共对象可以是有限域或环上的多项式。

[0097] 通过将密钥协商协议中的公共对象 a 绑定到由各方共享的上下文信息,可以将信道认证引入到标准的KEX和KEM协议中,例如Round5、Kyber、Frodo等。信道认证有助于避免MitM或冒充攻击。

[0098] 注意,在实施例,各方使用的参数 a 可以是秘密的。这与传统的密钥协商协议不同,在传统的密钥协商协议中,公共对象通常是公共参数。有利地,这进一步减少了想要破解密码系统的攻击者可用的信息。

[0099] 图1示意性地示出了KEX协议的实施例的示例。在图1-3中,时间从图的顶部到底部增加。

[0100] 图1中的KEX允许第一方和第三方就密钥达成一致。由于第一方和第三方交换了许多调和位,因此该密钥具有低失败概率。

[0101] 图1示出了被配置为与第二密码设备20通信的第一密码设备10。第一密码设备10被配置为执行密码操作10.1。

[0102] 设备10的密码操作10.1可以包括选择预先种子 σ 。例如,预先种子可以随机地生成。公共对象 a 可以部分地从预先种子导出。因此,可以通过预先种子来控制公共对象中的熵;例如,公共对象可以至少与预先种子一样随机。在图1和图2中,随机源被标记为\$。

[0103] 设备10的密码操作10.1可以包括根据预先种子 σ 和预先共享秘密 p 来计算最终种子 τ 。根据两个或多个输入(例如,在这种情况下,预先种子 σ 和预先共享秘密 p)计算最终种子 τ ,可以通过应用函数(例如种子函数,例如散列、密钥导出函数等)来完成。

[0104] 例如,预先共享秘密 p 可能已经在第二密码设备和第一密码设备之间预先共享。例如,可以通过出界通信信道在设备之间共享预先共享秘密 p 。例如,该协议可以被配置为通过第一通信信道(例如电子通信信道,例如有线或无线通信信道)在设备之间进行通信。预先共享秘密 p 可以以不同的方式通信,例如,通过与第一通信信道不同的第二通信信道。

[0105] 在第二通信信道的实施例中,例如由制造商在第一设备10和第二设备20之一或两者中预编程秘密 p 。例如,秘密 p 可以在第一设备10和第二设备20之一中预编程,或者在那里生成。例如,用户可以通过用户接口将秘密输入到第一和第二设备中的另一设备中。例如,秘密可以显示在显示器上,或者可以在互联网浏览器中可见,或者可以显示在设备上的贴纸上,之后,例如用户例如通过用户接口将秘密 p 输入(例如,键入)另一设备。为了根据多个输入(例如,根据预先种子 σ 和共享秘密 p)计算最终种子 τ ,可以应用散列函数,或密钥推导函数等。散列函数也可以应用于进一步的信息 z 。

[0106] 一旦计算了最终种子,操作10.1可以包括根据最终种子 τ 来计算公共对象 a 。例如,确定性随机数生成器可用于此目的。例如,公共对象 a 可以是矩阵或多项式,其系数是从最终种子 τ 随机计算的。在图1中,计算最终种子和生成公共对象的组合在函数 sd 中组合。例如,函数 sd 可以实现为散列和 $dbrg$ 的组合,例如,以将预先种子和其它输入组合成最终种子,并根据最终种子导出公共对象。

[0107] 在实施例中,公共对象、公钥和私钥包括一个或多个多项式。多项式的次数可以是,例如,至少128、至少256、至少512等。公共对象和/或私钥的系数可以是对至少 2^8 、至少 2^9 、至少 2^{10} 等的整数求模。私钥的系数可以是对至少 2^5 、至少 2^6 、至少 2^7 等的整数求模。

[0108] 操作10.1还可以包括获得与第一密码设备相关联的第一私钥 r 。

[0109] 私钥(也称为秘密密钥)可以被随机选择,例如从随机源中抽取,因为这可以例如通过进一步混淆对应公钥与公共对象之间的连接而增加协议的安全性。然而,没有必要为每个协议随机生成私钥,例如第一私钥 r 。在实施例中,由一方或双方使用新的私钥来计算

密钥。然而,可以重新使用私钥,例如,重新用于该特定通信方,或用于可以运行协议的多个密码设备。可以对私钥施加各种限制以减小其尺寸,例如,可以限制私钥中非零系数的数量。后者是可选的而不是必要的。

[0110] 一旦已经获得(例如生成,例如从存储设备(例如设备的本地存储设备)取回)第一私钥 r ,操作10.1包括根据第一私钥 r 计算第一公钥 b 。计算公钥包括将私钥与公共对象 a 相乘,例如,使用噪声乘法。

[0111] 第一公钥 b 和预先种子 σ 被传送到第二密码设备20。图1示出了从第一设备10到第二设备20的通信11.1。通信11.1可以包括第一公钥 b 和预先种子 σ 。

[0112] 图1示出了被配置为与第一密码设备10通信的第二密码设备20。第二密码设备20可以被配置为执行密码操作20.1。

[0113] 第二密码设备20被配置为接收从密码设备10传送的第一公钥 b 和预先种子 σ 。第二密码设备20被配置为例如从设备20的存储设备中取回共享秘密 p ,例如,以与上述相同的方式。

[0114] 操作20.1可以包括根据从第一密码设备10接收的预先种子 σ 和根据预先共享秘密 p 来计算最终种子,例如,通过应用与设备10相同的种子函数。操作20.1可以被配置为使得设备10和设备20得到相同的最终种子 τ 。操作20.1可以包括根据最终种子计算相同的公共对象 a 。操作20.1可以被配置为使得设备10和设备20得到相同的公共对象 a 。

[0115] 注意,不需要在第一设备10和第二设备20之间的通信信道(例如第一通信信道)上共享公共对象。此外,共享的信息(例如 σ, b)不足以计算公共对象。这意味着窃听者不知道所使用的公共对象。

[0116] 操作20.1可以包括获得与第二密码设备相关联的(一个或多个)第二私钥。作为设备10,有相同的选项来获得其,例如生成,例如随机生成它,例如取回它等。与第一密码设备相关联的第一公钥 b 是从第一设备10获得的,例如,接收。

[0117] 操作20.1可以包括根据第二私钥 s 来计算第二公钥 u 。可以以与第一公钥 b 相同的方式计算第二私钥 s ,例如,计算第二公钥 u 可以包括将第二私钥 s 与公共对象 a 相乘。

[0118] 操作20.1可以包括根据第一公钥 b 和第二私钥 s 来计算第二原始共享密钥 k ,有时表示为 k^* 。计算第二原始共享密钥可以包括在第二私钥 s 和第一公钥 b 之间的乘法,这可以是相同类型的乘法但不必是噪声乘法。

[0119] 第二公钥 u 被发送到第一设备10。利用第二公钥 u ,第一设备10可以计算与第二原始密钥几乎相同的第一原始密钥。有时,第一和第二原始密钥可能相等,但它们也可能不相等。为了减少在第一和第二原始密钥之间的潜在差异,可以向协议添加各种元素。例如,图1示出了使用了调和的示例。

[0120] 例如,在实施例,操作20.1可以包括为原始共享密钥的至少部分系数生成调和数据 h 。调和数据 h 可以包括允许减少分别在第一和第二设备处导出的第一原始密钥和第二原始密钥之间的差异的信息。

[0121] 最后,操作20.1可以包括根据第二原始共享密钥 k^* 来生成传输密钥 K 。这可能包括应用散列函数。

[0122] 第二公钥 u 和调和数据 h 被传送到第一设备10。图1示出了通信21.1。例如,通信21.1可以包括第二公钥 u 和调和数据 h 。

[0123] 第一密码设备10被配置为接收从第二密码设备20传送的第二公钥u和调和数据h。第一密码设备10可以被配置为执行密码操作10.2。

[0124] 设备10的密码操作10.2可以包括根据第二公钥u和第一私钥r计算第一原始共享密钥k'。这可以以与在第二设备20处相同的方式完成,但是使用不同的密钥,例如,计算第一原始共享密钥可以包括在第二公钥(u)和第一私钥(r)之间的乘法。结果是第一和第二原始密钥可能彼此接近。

[0125] 设备10的密码操作10.2可以包括将调和函数中的调和数据h应用于第一原始共享密钥k'中的至少部分系数。这样的结果是调和的第一原始密钥可能等于第二原始密钥。现在可以从调和的第一原始共享密钥(k')获得相同的传输密钥K。如果仅调和原始密钥的部分系数,则第一和第二设备可以使用调和的系数来计算传输密钥并且可以忽略未调和的系数。仍然存在小的变化,即两个设备不会得到相同的传输密钥,但可以管理这种概率,并在需要时降低该概率。

[0126] 密码操作10.1、20.1和10.2可以按该次序执行。

[0127] 在同一申请人于2016年11月4日向欧洲专利局提交的题目为“REACHING AGREEMENT ON A SECRET VALUE”、申请号为16197277.3的专利申请中解释了计算调和数据的可能方法;例如,在实施例中可以使用第7-10页上的方法进行调和。也可以采用在引用的专利申请中其它地方公开的变体。在该申请中,以下符号适用于以下三个函数:

[0128] 1、舍入函数 $\lfloor \cdot \rfloor_{B,b_h}$:对于 $q, b_h, B \in \mathbb{Z}, b_h \geq 1, B < \log_2 q - b_h$, 令

[0129] $\bar{B} = \log_2 q - B$ 。则,

[0130] $\lfloor \cdot \rfloor_{B,b_h}: v \rightarrow \lfloor 2^{-\bar{B}} \cdot v \rfloor \pmod{2^B}$

[0131] 直观上, $\lfloor v \rfloor_{B,b_h}$ 提取 $\{v + 2^{\log q - (B+b_h)}\}$ 的B个最高有效位,其中第二分量是舍入因子,以确保无偏舍入错误。B表示从符号v中提取的位数,并且 b_h 表示辅助数据位数。在实施例中,q可以是2的幂。

[0132] 2、交叉舍入函数 $\langle \cdot \rangle_{B,b_h}$:对于 $q, b_h, B \in \mathbb{Z}, b_h > 1, B < \log_2 q - b_h$, 令 $\bar{B} = \log_2 q - B$ 。则,

[0133] $\langle \cdot \rangle_{B,b_h}: v \rightarrow \lfloor 2^{-\bar{B}+b_h} \cdot v \rfloor \pmod{2^{b_h}}$

[0134] 直观上, $\langle v \rangle_{B,b_h}$ 提取v的 $(B+b_h)$ 个最高有效位的 b_h 个最低有效位。

[0135] 3、调和函数 $\text{rec}(w, b)$:

[0136] 对于 $q, b_h, B \in \mathbb{Z}, b_h \geq 1, B < \log_2 q - b_h, w \in \mathbb{Z}_q, b \in [0, 2^{b_h})$,

[0137] $\text{rec}(w, b) = \lfloor v \rfloor_{B,b_h}$

[0138] 其中,v是最接近w的元素,使得 $\langle v \rangle_{B,b_h} = b$ 。最近的元素w可以根据Lee距离取例如 $\min(|v-w|, q-|v-w|)$ 。

[0139] 这三个函数可以按系数应用于多项式或矩阵等。上面引用的调和函数在此用作示例。如上所述,也可以使用上面引用的申请中的调和函数。可以应用交叉舍入函数来获得调和数据,并应用舍入函数来获得被调和的数据。当调和数据稍后在调和函数中使用,调和

数据被恢复。换句话说： $rec(w, \langle v \rangle) = [v]$ ，假设 v 和 w 在彼此的阈值距离内。

[0140] 在实施例1中，第一和第二公钥、第一和第二私钥以及原始密钥是在有限域或环上的多个多项式，通过与多个共享多项式(a)的噪声乘法从私钥获得公钥。例如，多个多项式可用于其中晶格的元素是多项式的模块-晶格中。

[0141] 图2示意性地示出了KEM协议的实施例的示例。图2中图示的协议与图1的协议大致相似，不同之处在于原始密钥用于封装，并且在原始密钥之间可能出现的差异的概率以不同的方式降低。图2的协议的优点在于它允许第二方在给定第一方的公钥b的情况下封装他自己选择的随机密钥。这允许实现主动安全。

[0142] 在根据图1的实施例1中，第一设备10可以首先执行密码操作，这些可以是图1所示的操作10.1的实施例。从设备10到设备20的通信11.1可以与图1中的相同。

[0143] 图2然后可以在接收到预先种子 σ 和公钥b之后进行密码操作20.2。密码操作20.2可以与操作20.1相同，除了不计算调和数据。相反，操作20.2可以包括生成传输密钥K。图1和图2的不同在于，对于图2，可以控制最终传输密钥是什么，例如，第二设备20可以选择它。选择可能是随机生成的，但也可能是其它算法的结果。

[0144] 代替调和数据，通过应用封装函数，例如函数 ecp ，用第二原始共享密钥的至少一部分封装传输，从而获得封装数据c。

[0145] 封装数据c例如与第二公钥u一起被传送到第一密码设备。例如，第二设备20可以向第一设备10发送通信21.2。

[0146] 第一设备10可以被配置为接收从第二密码设备20传送的封装数据c，例如，连同第二公钥u。第一设备10可以被配置为执行密码操作10.3。操作10.3与操作10.2类似，除了使用封装而不是调和来减少第一与第二原始密钥之间的差异。

[0147] 例如，操作10.3可以包括使用第一原始共享密钥 k' 的至少部分对封装数据c进行解封装以获得传输密钥K。

[0148] 在实施例1中，传输密钥K是随机的和/或短暂的和/或对称的和/或独立于第一公钥(b)。

[0149] 例如，传输密钥K可以独立于第一私钥、第一公钥、第二私钥和第二公钥生成，即传输密钥K可以独立于第一和第二原始密钥。注意，原始密钥确实取决于公钥和私钥。例如，传输密钥可以至少部分随机地生成。独立的密钥更容易实现主动安全。计算密钥(例如私钥或传输密钥)的随机性可以从传统的随机数生成器(优选地，真正的随机数生成器)中获得。

[0150] 在实施例1中，公共对象和私钥是系数以 q 为模的 n 次多项式。公钥可以是以 p 为模的 n 次多项式。

[0151] 广泛的参数是可能的，通常受限于得到的密钥协商协议生成具有足够低的故障概率的足够大的密钥。后两个参数可以凭经验观察或从理论上计算。可接受的值取决于应用。

[0152] 可以结合图2使用的特别有利的KEM协议在NIST提案“Round5: KEM and PKE based on(Ring) Learning with Rounding, Thursday 28th March, 2019”中进行了描述，该提案通过引用包含在本文中。例如，第2.9.5和2.9.7节给出了适用于各种情况的示例性参数。例如，上面的论文提供了KEM协议的封装、纠错和其它细节的示例。

[0153] 例如，如图2所示，KEM协议可以定义在分圆环 $Z_q[x]/\Phi_{n+1}(x)$ 上，优选地具有 $n+1$ 个素数，例如，次数为 n 的多项式具有以 q 为模的系数。归约多项式可以是任意的，但第 $(n+1)$ 分

圆多项式 $\Phi_{n+1}(x) = x^n + \dots + x + 1$ 可能是有效的选择。公共对象A可以是 $d/n \times d/n$ 矩阵, 其条目在 $Z_q[x]/\Phi_{n+1}(x)$ 中。私钥可以是 $d/n \times \bar{n}$ 或 $d/n \times \bar{m}$ 维度的矩阵。

[0154] 例如, 可以使用以下参数:

[0155] d : 公共矩阵每行多项式系数的数量

[0156] n : 归约多项式的次数; 还指示是使用环 ($n > 1$) 还是非环 ($n = 1$) 实例化

[0157] h : 秘密矩阵的每列的非零多项式系数的数量

[0158] q, p, t, b : 舍入模数, 例如 $b | t | p | q$, 例如2的所有幂, 满足 $b < t < p < q$

[0159] b_bits : 在密文分量中每个符号的提取位数; $= 2^{b_bits}$,

[0160] κ : 安全参数; 传输密钥中的信息位数

[0161] $\bar{n}$: 发起者的秘密矩阵的列数

[0162] $\bar{m}$: 响应者的秘密矩阵的列数

[0163] 例如, 在实施例中, 人们可以选择: $d = 618, n = 618, h = 104, q = 2^{11}, p = 2^8, t = 2^4, b = 2^1, \kappa = 128, \bar{n} = 1, \bar{m} = 1$ 。

[0164] 为了进一步降低错误概率, 可以在封装之前将传输密钥编码在码字中。这可以使用以下附加参数。

[0165] f : 纠错码可纠正的位错误数

[0166] xe : 纠错码奇偶位数

[0167] μ : 密文分量中的符号数量 $\mu = \left\lceil \frac{\kappa + xe}{b_bits} \right\rceil$

[0168] 例如, 对于上述情况, 上述参数可能有: $f = 0, xe = 0, \mu = 128$ 。在实施例中, 可以具有 $\mu \leq \bar{n} \cdot \bar{m} \cdot n$ 和 $\mu \cdot b_bits \geq \kappa$ 。

[0169] 不同的实例化可以如下:

[0170] $d = 1186, n = 1, h = 712, q = 2^{15}, p = 2^{12}, t = 2^7, b = 2^4, \kappa = 256, \bar{n} = 8, \bar{m} = 8, f = 0, xe = 0, \mu = 64$ 。

[0171] 不同的实例化可以如下:

[0172] $d = 490, n = 490, h = 242, q = 2^{10}, p = 2^7, t = 2^3, b = 2^1, \kappa = 128, \bar{n} = 1, \bar{m} = 1, f = 5, xe = 190, \mu = 318$ 。

[0173] 与上述类似的参数可用于根据图1的协议。

[0174] 存在各种其它方式来减少第一和第二原始密钥之间的距离, 这些方式可以除了或替代关于图1和图2所示的那些方式而被采用。例如, 在实施例中, 使用封装和调和两者。在这种情况下, 人们可以使用调和的原始密钥进行封装。例如, 在计算调和和/或封装之前, 可以选择第二原始密钥的所谓可靠位, 例如, 最有可能在第一设备10处产生相同位的第二原始密钥的那些系数。然后可以将调和和/或封装应用于所选的可靠系数。可靠系数的索引可以例如在通信21.2中从设备20通信到设备10。

[0175] 下面给出了计算最终种子 τ 、预先种子 σ 和/或预先共享秘密 p 的各种示例。这些示例中的每个都可以并入本文描述的各种密钥协商协议中, 特别是图1和2的那些。

[0176] 例如, 在实施例中, 预先共享秘密可以包括预先共享口令。例如, 密码可以是字母数字字符序列或数字字符序列。例如, 预先共享秘密可以通过带外信道获得。

[0177] 例如,在实施例,可以以明文格式发送和接收预先种子 σ 。例如,设备10可以随机生成预先种子 σ ,并以明文格式(例如,未加密)将其发送到第二设备20。有趣的是,系统的安全性并未因此而受到影响。攻击者无法单独从预先种子 σ 中获取公共对象 a ,此外即使他可以,得到的传输密钥 K 系统的安全性也不依赖于公共对象 a 的保密性。

[0178] 例如,可以通过安装在第一设备10和第二设备20中的通信接口来发送和接收预先种子,该通信接口用于交换密钥协商协议的通信(例如消息),和/或用于在它们之间交换并且用传输密钥保护的后续通信。在实施例,不通过那些通信接口发送预先种子。

[0179] 例如,最终种子 τ 可能取决于比预先种子和预先共享秘密更进一步的信息。例如,进一步的信息可以包含于散列或密钥导出函数中。例如,可以根据来自第二密码设备和第一密码设备之间的网络连接的网络配置数据进一步计算最终种子。即使网络配置数据是公共数据,它仍然有助于减轻MitM攻击或冒充攻击,因为攻击者将需要跟踪进一步的信息。

[0180] 例如,进一步的信息可以包括第一和/或第二密码设备的网络地址。网络地址的示例是IP地址或MAC地址。

[0181] 例如,进一步的信息 z 可以包括网络连接的目的。例如,网络连接的目的可能是为特定应用执行通信。应用的名称可以包含在进一步的通信中。连接的目的可以从先前导出的信息中导出。例如,网络端口地址可用于导出目的。网络端口本身也可以是进一步信息的一部分。例如,密钥协商协议可能由于随后要执行的进一步算法而被执行;进一步算法的指示可以用作计算最终种子的进一步信息,并且可以稍后被验证以查看是否确实使用进一步算法或者拒绝与进一步信息不一致的算法。

[0182] 例如,进一步信息 z 可以包括一天中的时间,可能包括当前日期。例如,第一和第二设备可以首先执行同步协议以同步它们的时间,之后同步时间可以用作进一步的信息。例如,当前日期可以包含于进一步的信息中。

[0183] 例如,进一步的信息 z 可以包括交互计数器。交互计数器可以由第二密码设备20和第一密码设备10维护。例如,交互计数器可以至少每当导出共享密钥时增加。

[0184] 因此,可以通过从三个来源导出最终种子 τ 来实现对攻击的进一步抵抗:可以例如在通信11.1中共享的预先种子 σ ,预先共享秘密 p 和进一步信息。实际上,通过从两个来源的另一选择中导出最终种子 τ ,也可以获得具有不同属性的有利协议,例如:预先种子 σ 和进一步信息 z ,或者,例如,预先共享秘密 p 和进一步信息。

[0185] 进一步信息中使用的网络配置数据可以来自第一密码设备和第二密码设备之间的当前网络连接,和/或在进一步信息中使用的网络配置数据可以来自第一密码设备和第二密码设备之间的先前网络连接。

[0186] 例如,在实施例,如果预先共享秘密匹配,则获得成功的密钥协商。例如,共享秘密 p 可以是PIN或预先共享密钥(PSK)。如果双方知道预先共享的秘密,例如PIN或PSK,那么他们都能够推导出最终种子 τ ,并推导出公共对象 a 。例如, $\tau = \text{Hash}(p \parallel \sigma)$ 和 $a = \text{drbg}(\tau)$ 。一旦获得最终种子 τ ,就可以照常遵循使用种子的已知KEX或KEM协议。如果攻击正在进行,例如MitM或冒充,则KEX或KEM协议将不会导致共享对称密钥或允许适当的解封。稍后定期使用已建立的密钥将隐式确定双方是否共享相同的秘密 p 。隐式认证可以转换为显式认证。例如,通信11.1可以包括质询,并且通信21.1或21.2可以包括对应的响应。例如,质询可以是随机数,而响应可以是用传输密钥的加密。在导出传输密钥之后,设备10可以验证响应,

因此获悉设备20是否具有与其自己匹配的秘密 p 。质询也可以是隐式的,例如,质询可以是预定的字符串。

[0187] 图1和图2中的消息或以后的消息可以包括消息认证码或消息认证标签。如果它们可以被正确验证,则隐式认证可以转换为显式认证。如果它们无法被正确验证,则隐式缺少认证可以转换为显式缺少认证。

[0188] 注意,即使使用了短的共享秘密,例如,具有4个数字的PIN仅有10000个可能值,那么这种结构也确保了PIN不能轻易被暴力破解。原因在于即使秘密值 p 的数量有限(10000),该值也不会通过线路,使得攻击者无法导出使用的PIN。通过线路交换的值(公钥分量 b 和 u)是通过将公共对象 a 与 s 和 r 相乘获得的。由于 s 和 r 本身都是秘密,因此这些公钥分量无法轻松链接回共享秘密。相比之下,在传统算法中,密码的散列可能通过线路,当密码的熵很低时,这可能直接导致密码泄漏。另一优点在于任何一方都不会获悉另一方的共享秘密。原因在于公共对象不能从公钥的知识中推导出来。

[0189] 在实施例中,除了预先种子 σ 和预先共享秘密 p 之外,最终种子 τ 可能从进一步信息 z 推导出。该构造可用于建立双方之间的安全连接,例如,使用诸如IPSec的网络协议。例如,在实施例中,各方可以定期建立连接,然后进一步信息可以包括,例如:

[0190] -关于当前交换的信息,包括(1)第一方的当前IP地址;(2)IP连接的目的,例如以后会用到哪些其它协议;(3)一天中的时间;

[0191] -关于先前交换的信息,例如:(1)上次交换密钥的时间;(2)交换的目的。该信息可以是公开的,但它确实意味着如果攻击者要在冒充或MitM攻击中成功冒充双方,攻击者可能必须跟踪双方之间的状态。

[0192] -来自随机数信标的随机数,例如NIST随机信标。如果在进一步信息中使用了信标的最后公开的随机数,则第二方知道这是一次新的握手,而不是重放。

[0193] -关于当前连接的信息,例如IP地址。然后对应方将密钥交换绑定到该特定IP地址。这避免了混合和匹配攻击,在这种攻击中,通信的某些部分在不同的上下文中被重新使用。

[0194] -包括第一方打算使用的后续协议的信息,然后第二方可以尽早检查目的是否合适。尽早检查的能力意味着DOS攻击更加困难。

[0195] -关于先前密钥交换的信息。这迫使潜在攻击跟踪那些先前的交换以破坏协议。

[0196] 有趣的是,当使用预先共享的秘密 p 时,在给定公共分量 b 和 u 的情况下,攻击者无法恢复秘密上下文 p 。事实上,如果 p 的空间(例如安全参数的大小)很大,那么安全性就相当于找到散列函数输出的原像。因此,如果使用安全散列函数,则系统是安全的。然而,即使秘密 p 只有有限数量的状态,在极端情况下,只有2个可能的状态,那么安全性仍然等价于以下问题:假设公共 $(a_1, a_2, b) = (\text{hash}(\sigma, m), \text{hash}(\sigma, 1-m), m \cdot A_1 \cdot s + (1-m) \cdot A_2 \cdot s)$ 具有公开种子,秘密 $m=0$ 或 1 ,以及秘密 s ,找出 m ,或者换句话说,找出是否使用了 a_1 或 a_2 。在这个问题中, A_1 和 A_2 是可以从种子以已知方式导出的公共对象,例如,我们可以使用 $A_1 = \text{sd}(\sigma, m)$ 等。

[0197] LWE/R假设指出,很难将 $(A, b=A \cdot s)$ 与均匀随机区分开来。在上述问题中, $(A_1, b=A_1 \cdot s)$ 和 $(A_2, b=A_2 \cdot s)$ 都是LWE/R样本,难以与均匀区分开,因此难以彼此区分开。

[0198] 图3示意性地示出了在第一设备10和第二设备20之间的协议的实施例的示例。

[0199] 图3中示出了共享预先共享秘密 p 的出界通信13。出界通信13可以在设备10和20的

登记阶段31期间进行。例如,可以在该设备的制造期间执行出界通信13,例如,以使它们能够用于以后的通信。例如,可以在设备的制造期间部分地执行出界通信13,例如以使其能够用于以后的通信。稍后可以向设备中的另一个提供预先共享秘密。例如,出界通信可以由用户执行,例如,通过一个或两个设备上的用户接口手动执行。例如,可以通过设置设备的开关(例如,拨码开关)或通过另一接口来表示秘密,从而在设备之一(例如设备20)上设置预先共享秘密。秘密可以在另一设备上生成并在另一设备上设置。

[0200] 在稍后的密钥协商阶段32中,第一设备10和第二设备20根据实施例(例如关于图1或图2在本文描述的实施例)执行密钥协商协议。在密钥协商协议中,可以交换两个消息:密钥协商协议消息14和密钥协商协议消息15,例如,如本文所述。密钥协商协议中可能存在更多的消息。在密钥协商协议中,可以使用预先共享秘密 p 。

[0201] 在密钥协商阶段32结束时,两个设备可以具有传输密钥 K ,该传输密钥 K 至少相对于秘密 p 被隐式地认证。如果设备10和20不具有相同的共享,则至少在大多数情况下,在两个设备处导出的传输密钥 K 将不同。

[0202] 在实施例中,登记阶段31和密钥协商阶段32使用不同的通信信道,例如不同的通信介质,但它们可以使用不同的频率或不同的频带。

[0203] 在稍后的使用阶段33期间,可以使用在密钥协商阶段商定的传输密钥。例如,可以在设备10和20之间交换使用传输密钥 K 进行密码保护的消息,例如,消息可以用密钥 K 加密或者包括用密钥 K 计算出的认证标签(例如MAC)或者这两者。还可以用从密钥 K 导出的密钥来保护消息。图3示出了两个消息16和17,但是可能存在多于2个消息,例如,4个或更多等,或者一个消息等。消息的次序可能不同。

[0204] 例如,设备20可以被配置为用传输密钥 K 对消息 m 进行加密,并且将所述加密消息传送到第一密码设备10,或者反之亦然。设备10可以被配置为使用传输密钥 K 解密消息。

[0205] 传输密钥是从原始共享密钥导出的密钥。例如,传输密钥可以独立于原始共享密钥,例如在KEM协议中。在实施例中,用于加密的密钥可以是传输密钥和公钥的散列。例如,接收者的公钥。人们也可以用发送者的公钥进行散列,或者用两者。例如,传输密钥可以直接从原始共享密钥导出,例如通过对其进行散列。在实施例中,用于加密的密钥可以是原始密钥和公钥的散列。

[0206] 在密钥协商阶段32或使用阶段33期间,隐式认证可以转换为显式认证。例如,可以使用传输密钥来完成质询-响应协议,例如直接使用传输密钥或从其导出的密钥。

[0207] 有趣的是,质询-响应协议可能是隐式的。例如,在使用阶段33期间,消息可以作为保护的一部分进行认证。如果认证失败,这可能意味着消息被篡改或预先共享秘密 p 在设备之间不匹配。在这两种情况下,都不能信任通信并且可以采取适当的动作。在检测到问题时的适当动作可以包括,例如中止通信、启动新的密钥协商协议、发送警告消息(例如,电子邮件、警报等)。

[0208] 例如,在使用阶段33期间,可以将消息加密作为保护的一部分。如果消息包含可预测部分,例如预定字符串、报头,例如计数器等,则可在解密之后验证可预测部分。如果可预测部分在解密之后未能与预测匹配,则可以断定消息被篡改或预先共享秘密 p 在设备之间不匹配。在这种情况下可以采取适当的动作。

[0209] 一个有趣的应用是例如用网络配置数据供应设备。例如,考虑被配置为执行网络

通信的设备。例如,考虑被配置为配置设备进行网络通信的设备。例如,在个实施例中,被配置为执行网络通信的设备可以是设备20,并且配置设备可以是设备10,但也可以是相反的。配置设备可以是智能手机、膝上型计算机、计算机等。

[0210] 例如,对于登记阶段31,可以向设备20提供预先共享秘密。预先共享秘密被出界通信到设备10。例如,预先共享秘密可以被提供在设备的外部,并且由用户输入,或者被扫描,例如以扫描QR码、条形码等的形式。当预先共享秘密在设备10中可用时,例如通过合适的界面,例如用户接口、扫描界面。例如,可以使用NFC或蓝牙来共享预先共享秘密。例如,可以通过按下设备10和/或20上的按钮来发起交换。例如,可以在设备10和/或20上随机生成预先共享秘密。

[0211] 在密钥协商阶段32期间,设备10和20使用预先共享秘密来就传输密钥K达成一致。例如,密钥协商阶段可以使用不同的通信信道,例如Wi-Fi。

[0212] 在使用阶段33期间,设备10可以将使用传输密钥保护(例如加密)的网络配置数据发送到设备20。例如,传输可以使用与密钥协商阶段32相同的通信信道,例如Wi-Fi等。在接收到网络配置数据之后,设备20可以使用网络配置数据通过计算机网络发送和接收数据。网络配置数据可以包括网络密钥、证书、网络地址等。用传输密钥加密消息(例如网络配置数据)包括用传输密钥直接加密以及间接加密,在间接加密中,从用于直接加密消息的传输密钥导出进一步的密钥。例如,设备20可以是路由器。诸如上述协议的协议也可用于配置照明元件,例如灯具。

[0213] 有趣的是,实施例可以提供比使用例如预先共享秘密来直接保护通信更安全的传输密钥。即使预先共享秘密中的熵较低,本实施例提供的传输密钥仍然可以具有高的熵。

[0214] 例如,可以耦合一对蓝牙设备以建立安全且经认证的通信链接。就密钥协商协议所提供的机密强度而言,该链接是安全的,并且由于它们都使用相同的预先共享秘密而进行了认证。

[0215] 实施例也可以用于解决冒充攻击。例如,在常规协议中,例如,其中公共对象作为协议的一部分被固定或共享,攻击者可以从一侧重放消息。可能需要很长时间才能让第二方注意到有些错误。然而,当第二方接收到消息时,该方可能希望确保传入的消息确实来自特定来源。在实施例中,这可以通过在消息中包括变化元素来实现。例如,第二方可以在消息(例如在消息21.1或21.2)中包括质询(例如随机数),并将其发送到另一方以用传输密钥进行加密或认证。

[0216] 图4示意性地示出了根据实施例的密码系统301的示例。系统301包括第一密码设备300、第二密码设备350。例如,在诸如第一设备300和/或第二设备350的设备上的第一设备300和第二设备350。例如,设备300可以被配置为设备10,并且设备350可以被配置为设备20。

[0217] 第一设备300和第二设备350被配置为执行密码协议。它们能够将数据从一个设备传递到另一设备。

[0218] 例如,第一和第二设备可以被配置用于密钥协商协议,例如被设计为生成在两个设备之间共享的密钥,通常是对称密钥。共享密钥然后可以被设备用于受保护的通信,例如加密和/或认证的通信,例如,通过使用密钥来加密消息和/或计算消息的认证标签。

[0219] 在实施例中,设备300和设备350可以各自存储预先共享秘密p。例如,设备300和设

备350可以包括预先共享秘密单元(未单独示出)以获得和/或存储预先共享秘密。

[0220] 第一设备300、第二设备350可以分别包括存储接口、处理器和存储器中的一个或多个。第一设备300和第二设备350(例如系统301的各种设备)可以通过计算机网络391相互通信。计算机网络可以是互联网、内联网、LAN、WLAN等。计算机网络391可以是因特网。计算机网络可以全部或部分是有线的,和/或全部或部分是无线的。例如,计算机网络可以包括以太网连接。例如,计算机网络可以包括无线连接,例如Wi-Fi、ZigBee等。设备包括连接接口,其被布置为根据需要与系统301的其它设备进行通信。例如,连接接口可以包括连接器,例如有线连接器(例如以太网连接器),或无线连接器(例如天线,例如Wi-Fi、4G或5G天线)。例如,第一设备300和第二设备350可以分别包括通信接口305、355。计算机网络391可以包括附加元件,例如路由器、集线器等。

[0221] 第一设备300和第二设备350的执行可以在处理器中实现,例如处理器电路,其示例在本文中示出。第一设备300(特别是第一设备300的处理器)可以实现第一方10的功能。第二设备350(特别是第二设备350的处理器)可以实现第二方20的功能。例如,这些功能可以全部或部分地在存储在设备300或350处的计算机指令中实现,例如,在设备的电子存储器中,并且可由设备的微处理器执行。在混合实施例中,功能单元部分以硬件实现例如为协处理器(例如密码协处理器),部分以在设备300或350上存储和执行的软件实现。

[0222] 设备300和350可以包括存储接口以存储和/或取回消息,可能是加密消息。例如,存储接口可以在本地实现,例如作为到包含于设备中的存储器的接口,例如在相应设备的存储器中。存储接口还可以与离线(例如非本地)存储设备接口,例如云存储设备,例如位于另一设备中的诸如存储器或驱动器之类的存储设备。如果使用云存储设备,则设备也可以包括本地存储设备,例如存储器。例如,存储器可用于存储计算机编程指令、文件的临时存储等。

[0223] 在设备300和350的各种实施例中,可以从各种备选方案中选择通信接口。例如,接口可以是局域网或广域网(例如因特网)的网络接口、内部或外部数据存储设备的存储接口、应用接口(API)等。

[0224] 设备300和350可以具有用户接口,该用户接口可以包括公知的元素,例如一个或多个按钮、键盘、显示器、触摸屏等。用户接口可以被布置用于容纳发起密钥协商协议、响应密钥协商协议、发送加密消息等的用户交互。

[0225] 存储设备可以实现为电子存储器,例如闪存,或磁存储器,例如硬盘等。存储设备可以包括一起构成存储设备的多个离散存储器。存储设备也可以是临时存储器,例如RAM。

[0226] 通常,设备300和350均包括微处理器,该微处理器执行存储在设备300和350中的适当软件。例如,该软件可能已经被下载和/或存储在对应的存储器中,例如,诸如RAM的易失性存储器或诸如闪存的非易失性存储器。替代地,设备300和350可以全部或部分地在可编程逻辑中实现,例如作为现场可编程门阵列(FPGA)。设备300和350可以全部或部分地实现为所谓的专用集成电路(ASIC),例如,为其特定用途定制的集成电路(IC)。例如,电路可以在CMOS中实现,例如使用硬件描述语言(如Verilog、VHDL等)。

[0227] 在实施例中,设备300和350可以包括一个或多个电路以实现相应设备的一个或多个或所有功能。电路可以实现本文描述的对应该功能。电路可以是处理器电路和存储电路,处理器电路执行在存储电路中以电子表示的指令。

[0228] 处理器电路可以以分布方式实现,例如,作为多个子处理器电路。存储设备可以分布在多个分布式子存储设备上。存储器的一部分或全部可以是电子存储器、磁存储器等。例如,存储设备可以具有易失性和非易失性部分。部分存储设备可能是只读的。电路也可以是FPGA、ASIC等。

[0229] 第一设备300可以包括公钥/私钥生成器315,其被配置为生成第一私钥(r)和从第一私钥导出的第一公钥(b)。从私钥导出公钥可以使用公共对象(a)。例如,生成公钥可能涉及与公共对象相乘,和/或引入一种噪声,例如缩小乘法结果,添加噪声项等。私钥和公共对象可以是例如在有限域或环上的多项式或矩阵。

[0230] 第一设备300和第二设备350被配置为就共同对象 a 达成一致。例如,第一设备300和第二设备350可以被配置为交换可以从中计算出最终种子的数据,例如一个或多个预先种子 σ ,发送到和/或自第一设备300和第二设备350。例如,第一设备300和第二设备350可以被配置为维护也可以从中计算最终种子的公共数据,例如计数器、网络数据等。例如,第一设备300和第二设备350可以被配置为存储秘密数据,例如预先共享秘密 p 。例如,第一设备300和第二设备350可以被配置为例如从随机数信标获得公共数据。对于这些源中的一个或多个,设备计算公共的最终种子 τ 。对于要得到相同的最终种子 τ 的攻击者,他需要访问或跟踪相同的来源。设备300和350被配置为从公共的最终种子导出公共对象 a 。注意,攻击者不知道用于密钥协商的公共对象。

[0231] 第一私钥和公钥可以临时生成。例如,后者可以用于密钥协商协议,特别是当第一和第二设备使用另一种认证机制(例如带外机制,例如基于证书的认证等)来相互认证时。

[0232] 例如,通过通信接口305和355将第一公钥从第一设备300传送到第二设备350。这可以通过直接通信来完成。如果需要,还可以与第一公钥一起传送预先种子 σ 。例如,通过发送预先种子 σ ,可以计算出可以从中生成公共对象(a)的最终种子。

[0233] 第二设备350可以包括公钥获取器360。公钥也可以直接从第一设备获取,可能是出界的,例如在电子邮件中。公钥可以被存储直到需要。然而,也可以接收第一公钥以供立即使用,例如,用于密钥共享操作,例如,在这种情况下,可以临时生成第一公钥和/或公共对象。

[0234] 第二设备350可以包括公钥/私钥生成器365,其被配置为生成第二私钥(s)并根据第二私钥(s)生成第二公钥(u)。第二公钥使用与生成第一公钥相同的公共对象。第一和第二私钥对于它们各自的设备是私有的。在需要时,它们可以与受信任方共享,例如用于备份、密钥代管(key escrow)等。公钥和公共对象不一定是安全的秘密;虽然如此,它们中的一个或多个在需要时仍然对第一和第二设备私有。例如,第一公钥可能只与第二设备共享,反之亦然。

[0235] 例如,在消息的情况下,如果消息是从独立于公钥加密的应用(例如,金融或通信应用等)生成的,则可以获得独立生成。例如,可以通过随机生成来获得独立生成。

[0236] 第二设备350可以包括原始密钥生成器375。原始密钥生成器375被配置为从第一公钥(b)和第二私钥(s)生成第二原始共享密钥(k^*)。例如,原始密钥生成器375可以被配置为将噪声乘法应用于第一公钥和第二私钥。例如,噪声乘法取决于底层机制可以是乘法或求幂。第二设备350被配置为将其第二公钥传送到第一设备300。

[0237] 第一设备300可以包括原始密钥生成器325。原始密钥生成器325被配置为从第二

公钥(u)和第一私钥(r)生成第一原始共享密钥(k'),例如,通过应用噪声乘法。遗憾的是,对于噪声乘法,可能会发生第一和第二原始密钥彼此接近的情况,但不一定相同。这种情况发生的特定可能性取决于底层噪声乘法。在大多数应用中可能会接受不同原始密钥的某种可能性,但是,这种可能性有多大将取决于应用。但通常情况下,较低的可能性将是优选的。原始密钥可以与私钥和公钥具有相同的数学类型,例如多项式或矩阵。

[0238] 调和数据生成器385被配置为为原始共享密钥的指示系数生成调和数据(h)。调和数据包括允许减少在第一和第二设备处导出的第一和第二原始密钥之间的差异的信息。例如,应用调和数据可能导致第一和第二设备处的原始密钥的系数之间的差异(例如Lee距离)减小,从而增加两者将产生相同位的可能性。调和数据可以在原始共享密钥中的系数上计算。

[0239] 实现调和数据的一种方法是采用在作为关键位之后的系数的一个或多个(例如 b_h)位。例如,每个所选系数的调和位的数量可以是例如1或2。较少数量的调和位具有减少通信开销的优点。但是,较大数量的调和位是可能的。

[0240] 第二设备350可以包括封装器390。封装器390被配置为通过应用封装函数(例如XOR)来用密钥位封装密钥K。封装可以是一次性焊盘封装。例如,可以在本文描述的其它封装函数之一上使用XOR函数。

[0241] 第二设备被配置为传送第二公钥(u)、调和数据(h)和/或封装数据(c)。传送可以响应于接收到第一公钥,例如,在密钥协商的情况下,或者不是,例如,在公钥加密的情况下。

[0242] 第一设备300被配置为从第二设备接收第二公钥(u)、调和数据(h)和/或封装数据(c)。第一设备300可以包括调和单元335,调和单元335被配置为将调和函数中的调和数据(h)应用于第一原始共享密钥(k')中的系数,获得密钥位(k)。例如,可以使用调和位来调和系数,然后对系数进行采样以获得可靠位。第一设备300包括解封装单元340,其被配置为对封装数据(c)解封装以获得密钥K。在实施例,设备300和设备350仅包括调和和封装/解封装单元中的一个。在实施例,设备300和设备350包括减少原始密钥之间距离的其它方式。

[0243] 图5a示意性地示出了根据实施例的密码方法400的示例。例如,方法400可以与方法450一起使用。例如,方法400和450可以根据本文描述的实施例进行扩展或改变。第二密码方法(400)可以包括:

[0244] -与第一密码设备(10)通信(405),

[0245] -根据以下计算(410)最终种子:

[0246] -从第一密码设备(10)接收的预先种子,以及

[0247] -预先共享秘密,所述秘密在第二密码设备和第一密码设备之间预先共享,

[0248] -根据最终种子计算(415)公共对象(a),

[0249] -获得(420)与第一密码设备相关联的第一公钥(b),并且获得与第二密码设备相关联的第二私钥(s),

[0250] -根据第二私钥(s)计算(425)第二公钥(u),计算第二公钥(u)包括将第二私钥(s)与公共对象(a)相乘,

[0251] -根据第一公钥(b)和第二私钥(s)计算(430)第二原始共享密钥(k*),计算第二原始共享密钥包括在第二私钥(s)和第一公钥(b)之间的乘法,

[0252] -将第二公钥(u)传送(435)到第一设备。

[0253] 图5b示意性地示出了根据实施例的密码方法450的示例。第一密码方法(450)可以包括:

[0254] -与第二密码设备(20)通信(455),

[0255] -选择(460)预先种子并将该预先种子发送到第二密码设备(20),

[0256] -根据预先种子和预先共享秘密计算(465)最终种子,所述秘密在第二密码设备和第一密码设备之间预先共享,

[0257] -根据最终种子计算(470)公共对象(a),

[0258] -获得(475)与第一密码设备相关联的第一私钥(r),并根据第一私钥(r)计算第一公钥(b),计算第一公钥(b)包括将第一私钥(r)与公共对象(a)相乘,以及将第一公钥(b)传送到第二密码设备,

[0259] -从第二密码设备接收(480)第二公钥(u),

[0260] -根据第二公钥(u)和第一私钥(r)计算(485)第一原始共享密钥(k'),计算第一原始共享密钥包括在第二公钥(u)和第一私钥(r)之间的乘法。

[0261] 例如,方法400和450可以是计算机实现的方法。例如,方法的计算部分可以用计算机、计算电路等来计算。例如,可以使用通信接口来完成与密码设备的通信。例如,可以从电子存储设备(例如存储器、硬盘驱动器等)存储或取回参数、密钥等。密钥和/或公共对象可以用大于10字节、50字节、100字节等的数据来表示。

[0262] 执行该方法的许多不同方式都是可能的,这对于本领域技术人员来说是显而易见的。例如,可以按照所示次序执行这些步骤,但是也可以改变步骤的次序或者可以并行执行一些步骤。此外,在步骤之间可以插入其它方法步骤。插入的步骤可以代表诸如本文所述的方法的改进,或者可以与方法无关。此外,在开始下一步骤之前,给定的步骤可能尚未完全完成。

[0263] 方法的实施例可以使用软件来执行,该软件包括用于使处理器系统执行方法400和/或450的指令。软件可以仅包括由系统的特定子实体采取的那些步骤。软件可以存储在合适的存储介质中,例如硬盘、软盘、存储器、光盘等。软件可以作为信号沿着有线、或无线、或使用数据网络(例如因特网)而被发送。软件可以在服务器上下载和/或远程使用。可以使用被布置为配置可编程逻辑(例如,现场可编程门阵列(FPGA))以执行该方法的比特流来执行该方法的实施例。

[0264] 应当理解,当前公开的主题还扩展到计算机程序,特别是载体上或载体中的计算机程序,适于将当前公开的主题付诸实践。程序可以是源代码、目标代码、源与目标代码之间的代码的形式,例如部分编译的形式,或者任何其它适合用于实现该方法的实施例的形式。与计算机程序产品相关的实施例包括对应于所阐述的方法中的至少一个的每个处理步骤的计算机可执行指令。这些指令可以细分为子程序和/或存储在可以静态或动态链接的一个或多个文件中。涉及计算机程序产品的另一实施例包括对应于阐述系统和/或产品中至少一个的设备、单元和/或部分中的每一个的计算机可执行指令。

[0265] 图6a示出了根据实施例的具有可写部分1010的计算机可读介质1000,该可写部分1010包括计算机程序1020,该计算机程序1020包括用于使处理器系统执行密码方法的指令。计算机程序1020可以作为物理标记或通过计算机可读介质1000的磁化而体现在计算机

可读介质1000上。然而,任何其它合适的实施例也是可以想到的。此外,应当理解,虽然计算机可读介质1000在此被示为光盘,但是计算机可读介质1000可以是任何合适的计算机可读介质,例如硬盘、固态存储器、闪存等,并且可能是不可记录的或可记录的。计算机程序1020包括用于使处理器系统执行所述密码方法的指令。

[0266] 图6b示出了根据密码设备的实施例的处理器系统1140的示意图。处理器系统包括一个或多个集成电路1110。一个或多个集成电路1110的架构在图6b中示意性地示出。电路1110包括处理单元1120,例如CPU,用于运行计算机程序组件以执行根据实施例的方法和/或实现其模块或单元。电路1110包括用于存储编程代码、数据等的存储器1122。存储器1122的一部分可以是只读的。电路1110可以包括通信元件1126,例如天线、连接器或两者等。电路1110可以包括专用集成电路1124,用于执行该方法中定义的部分或全部处理。处理器1120、存储器1122、专用IC 1124和通信元件1126可以经由互连1130(例如总线)彼此连接。处理器系统1110可以被布置用于分别使用天线和/或连接器进行接触式和/或非接触式通信。

[0267] 例如,在实施例中,处理器系统1140(例如密码设备)可以包括处理器电路和存储器电路,处理器被布置为执行存储在存储器电路中的软件。例如,处理器电路可以是Intel Core i7处理器、ARM Cortex-R8等。在实施例中,处理器电路可以是ARM Cortex M0。存储器电路可以是ROM电路,或非易失性存储器,例如闪存。存储器电路可以是易失性存储器,例如SRAM存储器。在后一种情况下,设备可以包括非易失性软件接口,例如硬盘驱动器、网络接口等,被布置用于提供软件。

[0268] 虽然设备1140被示为包括每个所描述组件中的一个,但是在各种实施例中可以复制各种部件。例如,处理单元1120(例如处理器1120)可以包括多个微处理器,这些微处理器被配置为独立地执行本文描述的方法或者被配置为执行本文描述的方法的步骤或子例程,使得多个处理器协作以实现本文所描述的功能。此外,在设备1140在云计算系统中实现的情况下,各种硬件部件可以属于单独的物理系统。例如,处理器1120可以包括第一服务器中的第一处理器和第二服务器中的第二处理器。

[0269] 应当注意,上述实施例示出了当前公开的主题而不是限制,本领域技术人员能够设计出许多替代实施例。

[0270] 在权利要求中,置于括号之间的任何参考标记不应被解释为限制权利要求。动词“包括”及其词形变化的使用不排除存在不同于权利要求中所述的元件或步骤。元件前面的词“一”或“一个”不排除存在多个这种元件。诸如“至少一个”的表达在元件列表之前表示从列表中选择所有元件或元件的任何子集。例如,表述“A、B和C中的至少一个”应理解为包括仅A、仅B、仅C、A和B两者、A和C两者、B和C两者或全部A、B和C。当前公开的主题可以通过包括若干不同元件的硬件以及通过适当编程的计算机来实现。在列举若干部分的设备权利要求中,这些部分中的若干部分可以由同一硬件项目来体现。在相互不同的从属权利要求中叙述某些措施这一事实并不表示不能有利地利用这些措施的组合。

[0271] 以下编号条款包括预期和非限制性的示例:

[0272] 条款1、第二密码设备(20),包括:

[0273] -通信接口,其被配置为与第一密码设备(10)通信,

[0274] -处理器,其被配置为:

- [0275] -根据以下来计算最终种子:
- [0276] -从第一密码设备 (10) 接收的预先种子,以及
- [0277] -预先共享秘密,所述秘密在所述第二密码设备与所述第一密码设备之间预先共享,
- [0278] -根据所述最终种子来计算公共对象 (a),
- [0279] -获得与所述第一密码设备相关联的第一公钥 (b),并且获得与所述第二密码设备相关联的第二私钥 (s),
- [0280] -根据所述第二私钥 (s) 来计算第二公钥 (u),计算所述第二公钥 (u) 包括将所述第二私钥 (s) 与所述公共对象 (a) 相乘,
- [0281] -根据所述第一公钥 (b) 和所述第二私钥 (s) 计算第二原始共享密钥 (k*),计算所述第二原始共享密钥包括所述第二私钥 (s) 与所述第一公钥 (b) 之间的乘法,
- [0282] -将所述第二公钥 (u) 传送到所述第一设备。
- [0283] 2、第一密码设备 (10),包括:
- [0284] -通信接口,其被配置为与第二密码设备 (20) 通信,
- [0285] -处理器,其被配置为:
- [0286] -选择预先种子并将所述预先种子发送到所述第二密码设备 (20),
- [0287] -根据以下来计算最终种子:
- [0288] -所述预先种子和所述预先共享秘密,所述秘密在所述第二密码设备与所述第一密码设备之间预先共享,
- [0289] -根据所述最终种子来计算公共对象 (a),
- [0290] -获得与所述第一密码设备相关联的第一私钥 (r) 并根据所述第一私钥 (r) 来计算所述第一公钥 (b),计算所述第一公钥 (b) 包括将所述第一私钥 (r) 与所述公共对象 (a) 相乘,并将所述第一公钥 (b) 传送到所述第二密码设备,
- [0291] -从所述第二密码设备接收第二公钥 (u),
- [0292] -根据所述第二公钥 (u) 和所述第一私钥 (r) 来计算第一原始共享密钥 (k'),计算所述第一原始共享密钥包括在所述第二公钥 (u) 与所述第一私钥 (r) 之间的乘法。
- [0293] 条款3、如前述条款中的任一项所述的第二密码设备 (20) 或第一密码设备 (10),其中,预先共享秘密包括预先共享口令。
- [0294] 条款4、如前述条款中的任一项所述的第二密码设备 (20) 或第一密码设备 (10),其中,以明文格式发送和接收所述预先种子。
- [0295] 条款5、如前述条款中的任一项所述的第二密码设备 (20) 或第一密码设备 (10),其中,所述预先种子通过通信接口发送和接收,但是所述预先共享秘密不通过通信接口发送和接收。
- [0296] 条款6、如前述条款中的任一项所述的第二密码设备 (20) 或第一密码设备 (10),其中,所述最终种子还根据来自所述第二密码设备和所述第一密码设备之间的网络连接的网络配置数据来计算。
- [0297] 条款7、如前述条款中的任一项的第二密码设备 (20) 或第一密码设备 (10),其中,所述最终种子根据以下计算:
- [0298] -第一和/或第二密码设备的网络地址,

- [0299] -网络连接的目的,
- [0300] -一天中的时间,
- [0301] -交互计数器,所述交互计数器由所述第二密码设备(20)和所述第一密码设备(10)维护并且至少每当导出共享密钥时增加。
- [0302] 条款8、如前述条款中的任一项所述的第二密码设备(20)或第一密码设备(10),其中,
- [0303] -所述第二密码设备(20)的所述处理器被配置为:
- [0304] -生成传输密钥(K),
- [0305] -通过应用封装函数,用第二原始共享密钥的至少部分来封装所述传输密钥(K),获得封装数据(c),
- [0306] -将所述封装数据(c)传送到第一密码设备,并且
- [0307] -所述第一密码设备(10)的所述处理器被配置为:
- [0308] -从所述第二设备接收封装数据(c),
- [0309] -使用所述第一原始共享密钥(k')的至少部分对所述封装数据(c)解封装以获得传输密钥。
- [0310] 条款9、如前述条款中的任一项所述的第二密码设备(20)或第一密码设备(10),其中,
- [0311] -所述第二密码设备(20)所述的处理器被配置为:
- [0312] -针对所述原始共享密钥的所述系数中的至少部分生成调和数据(h),所述调和数据包括允许减少在所述第一设备和所述第二设备处导出的第一原始密钥和所述第二原始密钥之间的差异的信息,
- [0313] -根据所述第二原始共享密钥(k*)来生成传输密钥(K),
- [0314] -将所述调和数据(h)传送到所述第一设备,并且
- [0315] -所述第一密码设备(10)的所述处理器被配置为:
- [0316] -从所述第二设备接收调和数据(h),
- [0317] -将调和函数中的所述调和数据(h)应用所述于第一原始共享密钥(k')的所述系数中的至少部分,
- [0318] -根据经调和的第一原始共享密钥(k')来生成传输密钥(K)。
- [0319] 条款10、如前述条款中的任一项所述的第二密码设备(20)或第一密码设备(10),其中,在计算所述第一公钥(b)和所述第二公钥(u)时与所述公共对象(a)的所述相乘是噪声乘法。
- [0320] 条款11、如前述条款中的任一项所述的第二密码设备或第一密码设备,其中:
- [0321] -所述第二密码设备的所述处理器被配置为利用所述传输密钥对消息(m)进行加密,并且将所加密的消息传送到所述第一密码设备,所述第一密码设备的处理器被配置为利用所述传输密钥对所加密的消息进行解密,并验证消息(m),和/或
- [0322] -所述第一密码设备的所述处理器被配置为用所述传输密钥对消息(m)进行加密,并将所加密的消息传送到所述第二密码设备,所述第二密码设备的所述处理器被配置为利用所述传输密钥对所加密的消息进行解密,并且验证消息(m)。
- [0323] 条款12、如前述条款中的任一项所述的第二密码设备或第一密码设备,其中,所述

传输密钥是随机的、和/或短暂的和/或对称的和/或独立于所述第一公钥(b)。

[0324] 条款13、如前述条款中的任一项所述的第二密码设备或第一密码设备,其中,

[0325] -所述第一和第二公钥、所述第一和第二私钥、所述第一和第二原始密钥以及所述公共对象是有限域或环上的矩阵,

[0326] -所述第一和第二公钥、所述第一和第二私钥、所述第一和第二原始密钥以及公共对象是有限域或环上的多项式。

[0327] 条款14、如前述条款中的任一项所述的第二密码设备或第一密码设备,其中,网络配置数据是利用所述传输密钥加密发送的。

[0328] 条款15、第二密码方法(400),包括

[0329] -与第一密码设备(10)通信(405),

[0330] -根据以下来计算(410)最终种子

[0331] -从所述第一密码设备(10)接收的预先种子,以及

[0332] -预先共享秘密,所述秘密在所述第二密码设备与所述第一密码设备之间预先共享,

[0333] -根据所述最终种子来计算(415)公共对象(a),

[0334] -获得(420)与所述第一密码设备相关联的第一公钥(b),并且获得与所述第二密码设备相关联的第二私钥(s),

[0335] -根据所述第二私钥(s)计算(425)第二公钥(u),计算所述第二公钥(u)包括将所述第二私钥(s)与所述公共对象(a)相乘,

[0336] -根据所述第一公钥(b)和所述第二私钥(s)计算(430)第二原始共享密钥(k*),计算所述第二原始共享密钥包括所述第二私钥(s)与第一公钥(b)之间的乘法,

[0337] -将所述第二公钥(u)传送(435)到所述第一设备。

[0338] 条款16、第一密码方法(450)包括:

[0339] -与所述第二密码设备(20)通信(455),

[0340] -选择(460)预先种子并将所述预先种子发送到所述第二密码设备(20),

[0341] -根据以下来计算(465)所述最终种子:所述预先种子和所述预先共享秘密,所述秘密在所述第二密码设备与所述第一密码设备之间预先共享,

[0342] -根据所述最终种子来计算(470)公共对象(a),

[0343] -获得(475)与所述第一密码设备相关联的第一私钥(r)并且根据所述第一私钥(r)来计算第一公钥(b),计算所述第一公钥(b)包括将所述第一私钥(r)与所述公共对象(a)相乘,并且将所述第一公钥(b)传送到所述第二密码设备,

[0344] -从所述第二密码设备接收(480)第二公钥(u),

[0345] -根据所述第二公钥(u)和所述第一私钥(r)来计算(485)第一原始共享密钥(k'),计算所述第一原始共享密钥包括在所述第二公钥(u)与所述第一私钥(r)之间的乘法。

[0346] 条款17、一种瞬态或非瞬态计算机可读介质(1000),包括表示指令的数据(1020),所述指令在由处理器系统运行时使所述处理器系统执行根据条款14和/或15所述的方法。

[0347] 在权利要求中,括号中的标记是指示例性实施例的附图中的附图标记或实施例的公式,从而增加了权利要求的可理解性。这些标记不应被解释为限制权利要求。

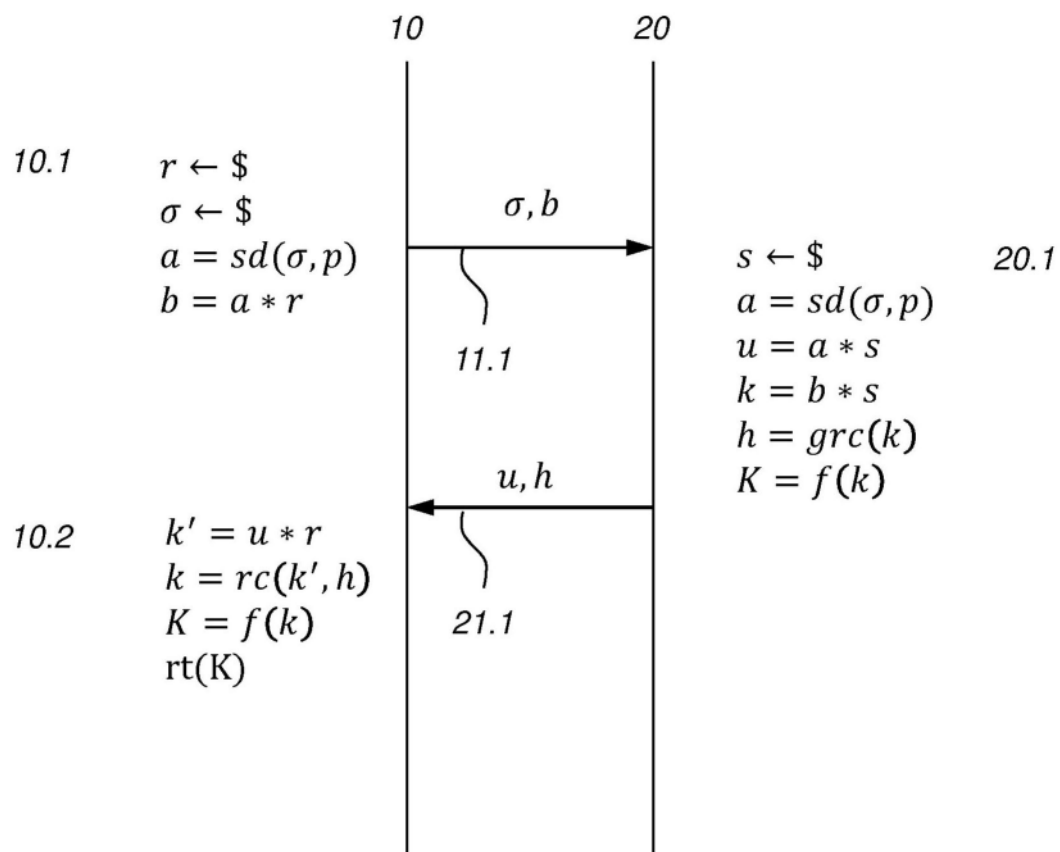


图1

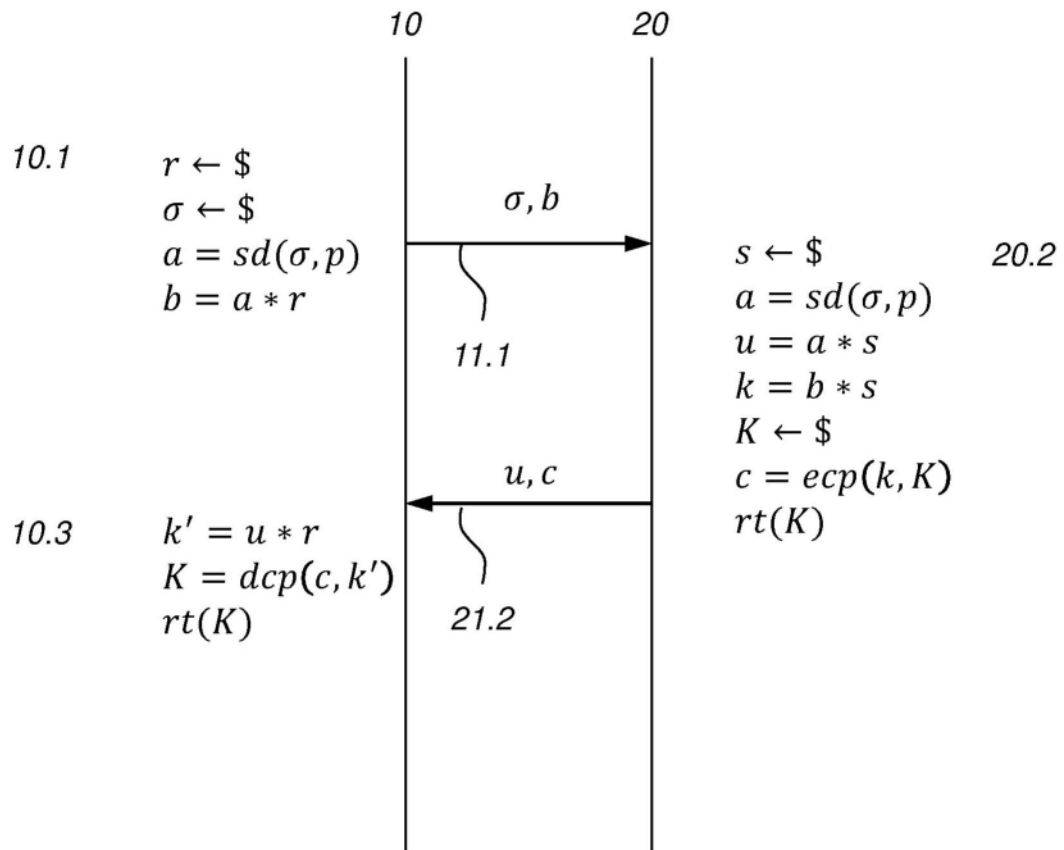


图2

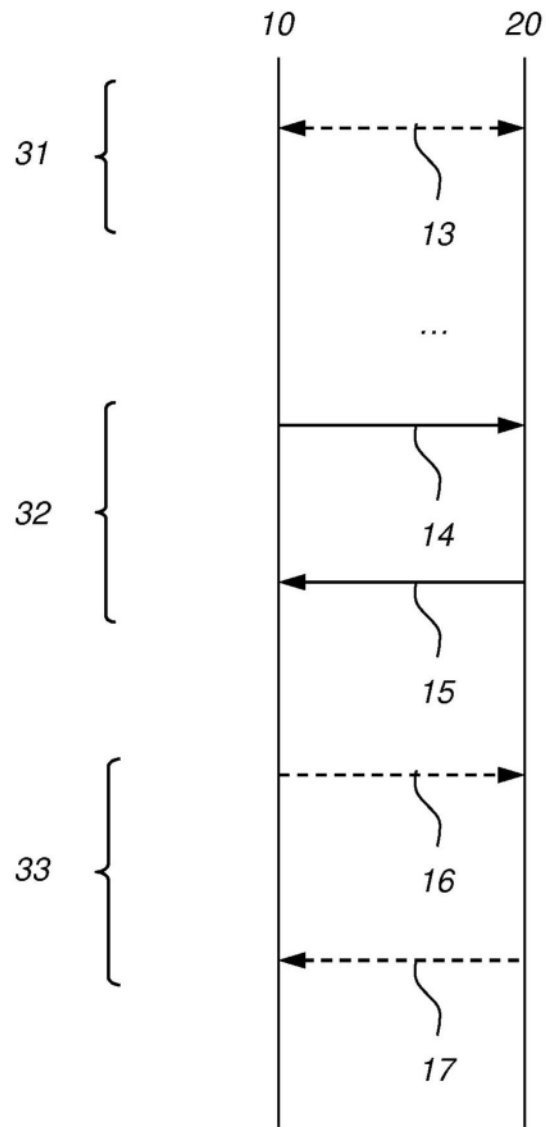
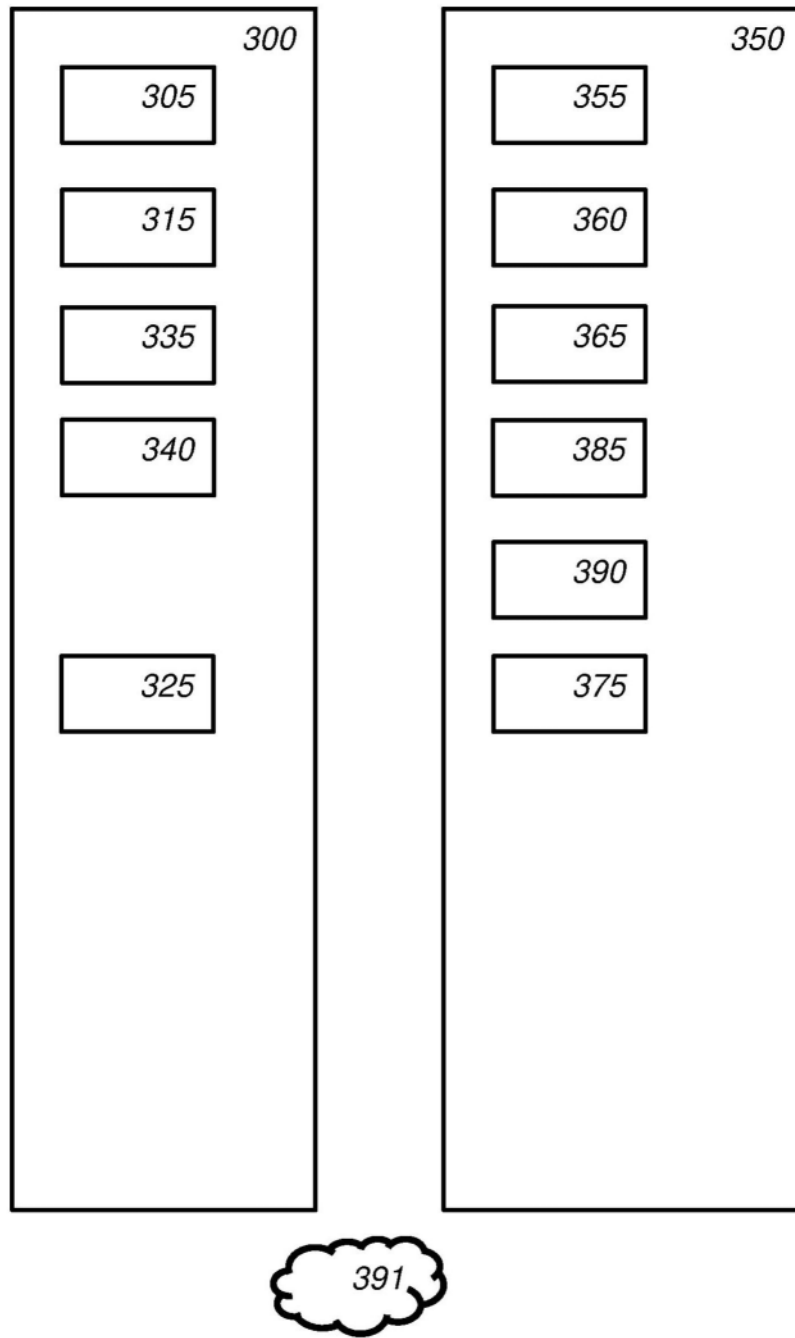


图3



301

图4

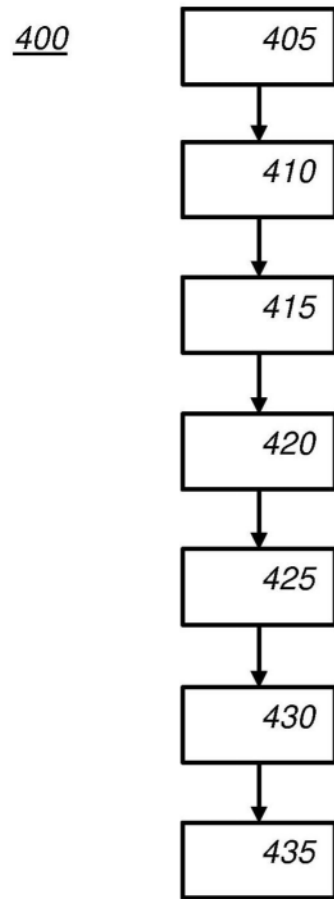


图5a

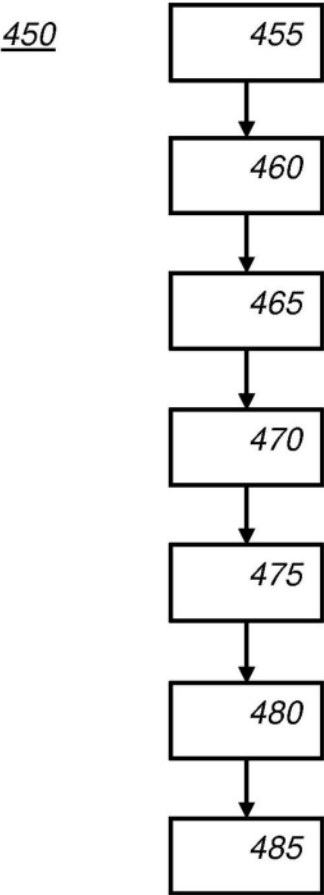


图5b

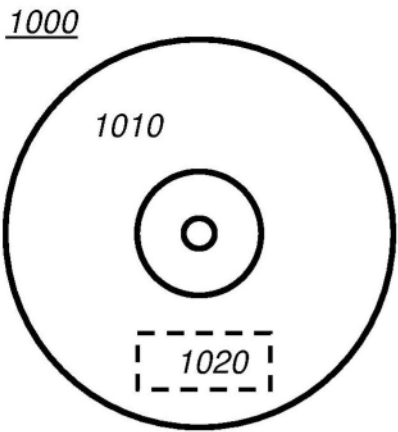


图6a

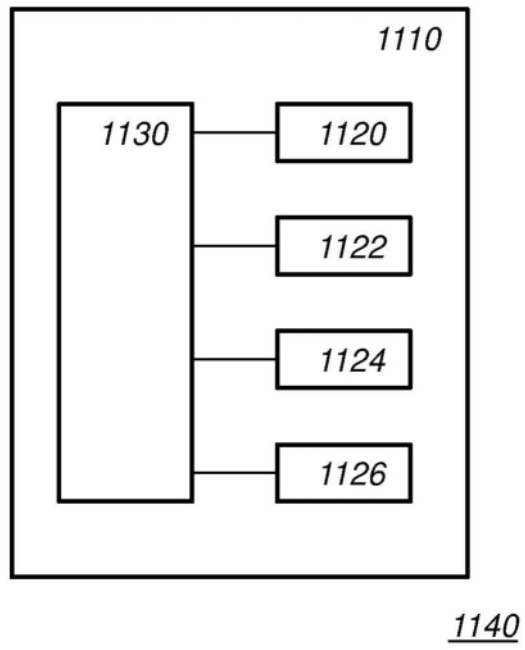


图6b