



(12) 发明专利

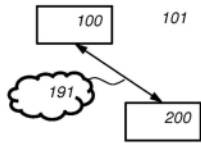
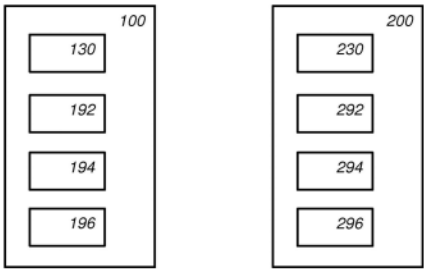
(10) 授权公告号 CN 112997448 B

(45) 授权公告日 2024. 12. 24

(21) 申请号 201980074156.5	(72) 发明人 O • 加西亚莫尔琼 S • 巴塔查里亚 L • M • G • M • 托尔胡伊泽恩
(22) 申请日 2019.09.02	
(65) 同一申请的已公布的文献号 申请公布号 CN 112997448 A	(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
(43) 申请公布日 2021.06.18	
(30) 优先权数据 18194118.8 2018.09.12 EP	(51) Int.Cl. H04L 9/08 (2006.01) H04L 9/30 (2006.01)
(85) PCT国际申请进入国家阶段日 2021.05.11	(56) 对比文件 S Bhattacharya.Round5: KEM and PKE based on GLWR .IACR Cryptology eprint archive 2018.2018,参见第1.1.3-1.9.8节.
(86) PCT国际申请的申请数据 PCT/EP2019/073327 2019.09.02	审查员 曹彦
(87) PCT国际申请的公布数据 W02020/053013 EN 2020.03.19	
(73) 专利权人 皇家飞利浦有限公司 地址 荷兰艾恩德霍芬	权利要求书5页 说明书27页 附图10页

(54) 发明名称
具有减小的公钥大小的公钥/私钥系统

(57) 摘要
一些实施例针对公钥加密设备 (20) 和私钥解密设备 (10)。公钥加密设备被配置为计算第二公钥矩阵 (u)，第二公钥矩阵 (u) 具有比私钥解密设备的第一公钥矩阵 (b) 少的矩阵元素。这减少了公钥加密设备一侧的计算需求和带宽需求。



1. 一种公钥加密设备(20), 其中, 在加密阶段期间, 第二公钥矩阵(u)的第二维度($\bar{m}$)是能配置的, 所述公钥加密设备包括:

通信接口, 其被配置为与私钥解密设备(10)通信;

处理器, 其被配置为:

获得与所述私钥解密设备相关联的第一公钥矩阵(b),

获得传输密钥(K)的密钥大小,

根据所述密钥大小来生成所述传输密钥(K),

通过相应地选择第二私钥矩阵(s)的第二维度($\bar{m}$)的值来确定第二私钥矩阵(s)的矩阵大小以应对所述密钥大小的所述传输密钥的掩蔽, 所述第二私钥矩阵(s)的第二维度($\bar{m}$)等于所述第二公钥矩阵(u)的第二维度($\bar{m}$),

根据所述矩阵大小来生成所述第二私钥矩阵(s), 并且根据所述第二私钥矩阵(s)来计算所述第二公钥矩阵(u),

根据所述第二私钥矩阵(s)和所述第一公钥矩阵(b)来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矩阵(s)与所述第一公钥矩阵(b)之间的矩阵相乘,

利用所述第二原始共享密钥的至少部分来掩蔽所述传输密钥(K),

将对所述密钥大小和/或所述矩阵大小的指示、所述第二公钥矩阵(u)以及经掩蔽的传输密钥(c)传送到所述私钥解密设备。

2. 根据权利要求1所述的公钥加密设备, 其中,

所述公钥加密设备的处理器被配置为与所述私钥解密设备执行握手, 包括:

从所述私钥解密设备接收对所述私钥解密设备的至少两个第一公钥矩阵的至少两个指示, 所述两个第一公钥矩阵具有不同的大小,

通过以下操作来选择第一公钥矩阵: 确定所述公钥加密设备的密钥高速缓存是否包括所述两个第一公钥矩阵中的较大者, 并且如果是这样, 则选择较大的第一公钥矩阵,

将对所选择的第一公钥矩阵的指示发送到所述私钥解密设备, 如果该第一公钥矩阵在所述密钥高速缓存中不可用, 则请求该第一公钥矩阵, 所述传输密钥(K)是利用所选择的第一公钥矩阵来封装的。

3. 根据权利要求1和2中的任一项所述的公钥加密设备, 其中,

所述第二私钥矩阵(s)具有比所述第一公钥矩阵(b)少的矩阵元素, 并且/或者

所述第二公钥矩阵(u)具有比所述第一公钥矩阵(b)少的矩阵元素, 并且/或者

所述第二公钥矩阵(u)具有比第一私钥矩阵(r)少的矩阵元素。

4. 根据权利要求3所述的公钥加密设备, 其中,

所述第二公钥矩阵(u)具有第一系统维度(d)和第二维度($\bar{m}$), 所述第一公钥矩阵(b)具有所述第一系统维度(d)和第二维度($\bar{n}$), 所述第二公钥矩阵(u)的第二维度($\bar{m}$)小于所述第一公钥矩阵(b)的第二维度($\bar{n}$)。

5. 根据权利要求4所述的公钥加密设备, 其中,

所述第二公钥矩阵(u)的第二维度($\bar{m}$)至多是所述第一公钥矩阵(b)的第二维度($\bar{n}$)的一半, 并且/或者

其中,所述第二公钥矩阵(u)的第二维度($\bar{m}$)为1。

6. 根据权利要求3所述的公钥加密设备,其中,

所述公钥加密设备的处理器被配置为:

获得与所述第一公钥矩阵(b)相关联的公共矩阵(a),并且其中,

计算所述第二公钥矩阵(u)包括所述第二私钥矩阵与所述公共矩阵(a)之间的噪声矩阵相乘,所述公共矩阵在所述公钥加密设备与所述私钥解密设备之间被共享。

7. 根据权利要求6所述的公钥加密设备,其中,所述噪声矩阵相乘包括从q个元素缩放到p个元素,其中, $\log_2 p / \log_2 q \leq 0.85$,

其中,所述公钥加密设备被配置为:

针对所述第二原始共享密钥的所述至少部分生成对帐数据(h),所述对帐数据包括允许减少在所述公钥加密设备和所述私钥解密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,并且将所述对帐数据(h)传送到所述私钥解密设备,

生成用于所述传输密钥的奇偶校验位,所述传输密钥和所述奇偶校验位根据纠错码来形成码字,掩蔽所述传输密钥包括封装所述码字。

8. 根据权利要求1和2中的任一项所述的公钥加密设备,其中,

所述公钥加密设备的处理器被配置为:至少基于所述传输密钥来导出最终密钥,利用所述最终密钥对消息(m)进行加密,并且将经加密的消息传送到所述私钥解密设备。

9. 根据权利要求1和2中的任一项所述的公钥加密设备,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矩阵(b)。

10. 根据权利要求1和2中的任一项所述的公钥加密设备,其中,

所述公钥加密设备的处理器被配置为:计算帮助者数据以减少在所述私钥解密设备处获得所述传输密钥时的错误率。

11. 根据权利要求7所述的公钥加密设备,其中,

所述第二原始密钥是矩阵,掩蔽所述传输密钥(K)包括:将所述传输密钥的位与第二原始密钥矩阵的元素的至少部分的最高有效部分相加,并且丢弃所述第二原始密钥矩阵的元素的至少部分的零或更多个最低有效位。

12. 根据权利要求1和2中的任一项所述的公钥加密设备,其中,

所述公钥加密设备的处理器被配置为:从所述传输密钥导出所述第二私钥矩阵。

13. 根据权利要求1和2中的任一项所述的公钥加密设备,其中,

所述公钥加密设备的处理器被配置为:从公钥数据库获得所述第一公钥矩阵。

14. 根据权利要求7所述的公钥加密设备,其中,

所述第一公钥矩阵和所述第二公钥矩阵、所述第一私钥矩阵和所述第二私钥矩阵以及所述第一原始密钥和所述第二原始密钥是有限域或环上的矩阵。

15. 一种密码系统,包括:

根据权利要求1所述的公钥加密设备(20);以及

私钥解密设备(10),其包括:

通信接口,其被配置为与公钥加密设备(20)通信;

处理器,其被配置为:

生成第一私钥矩阵(r),并且根据所述第一私钥矩阵(r)来计算第一公钥矩阵(b),并且

允许将所述第一公钥矩阵 (b) 传送到所述公钥加密设备,

从所述公钥加密设备接收对密钥大小和/或矩阵大小的指示、第二公钥矩阵 (u) 和经掩蔽的传输密钥 (c), 其中, 在加密阶段期间, 在所述公钥加密设备处, 所述第二公钥矩阵 (u) 的第二维度 ($\bar{m}$) 是能配置的,

根据所述第二公钥矩阵 (u) 和所述第一私钥矩阵 (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所述第二公钥矩阵 (u) 与所述第一私钥矩阵 (r) 之间的矩阵相乘, 并且

使用所述第一原始共享密钥 (k') 的至少部分, 根据接收到的大小对经掩蔽的传输密钥 (c) 进行解掩蔽, 以获得传输密钥。

16. 根据权利要求15所述的密码系统, 其中,

所述私钥解密设备的处理器被配置为与所述公钥加密设备执行握手, 包括:

将对所述私钥解密设备的至少两个第一公钥矩阵的至少两个指示发送到所述公钥加密设备, 所述两个第一公钥矩阵具有不同的大小,

从所述公钥加密设备接收对所选择的第一公钥矩阵的指示, 如果接收到对所选择的第一公钥矩阵的请求, 则发送所选择的第一公钥矩阵, 所述传输密钥 (K) 是利用所选择的第一公钥矩阵来解封装的。

17. 根据权利要求15和16中的任一项所述的密码系统, 其中,

所述第二私钥矩阵 (s) 具有比所述第一公钥矩阵 (b) 少的矩阵元素, 并且/或者
所述第二公钥矩阵 (u) 具有比所述第一公钥矩阵 (b) 少的矩阵元素, 并且/或者
所述第二公钥矩阵 (u) 具有比所述第一私钥矩阵 (r) 少的矩阵元素。

18. 根据权利要求17所述的密码系统, 其中,

所述第二公钥矩阵 (u) 具有第一系统维度 (d) 和第二维度 ($\bar{m}$), 所述第一公钥矩阵 (b) 具有所述第一系统维度 (d) 和第二维度 ($\bar{n}$), 所述第二公钥矩阵 (u) 的第二维度 ($\bar{m}$) 小于所述第一公钥矩阵 (b) 的第二维度 ($\bar{n}$)。

19. 根据权利要求18所述的密码系统, 其中,

所述第二公钥矩阵 (u) 的第二维度 ($\bar{m}$) 至多是所述第一公钥矩阵 (b) 的第二维度 ($\bar{n}$) 的一半, 并且/或者

其中, 所述第二公钥矩阵 (u) 的第二维度 ($\bar{m}$) 为1。

20. 根据权利要求15和16中的任一项所述的密码系统, 其中,

所述私钥解密设备的处理器被配置为:

生成公共矩阵 (a), 并且其中,

计算所述第一公钥矩阵 (b) 包括所述第一私钥矩阵 (r) 与所述公共矩阵 (a) 之间的噪声矩阵相乘, 所述公共矩阵 (a) 在所述公钥加密设备与所述私钥解密设备之间被共享, 所述第一公钥矩阵 (b) 与所述公共矩阵 (a) 相关联。

21. 根据权利要求20所述的密码系统, 其中,

所述私钥解密设备被配置为:

针对所述第一原始共享密钥 (k') 的所述至少部分接收对帐数据 (h), 所述对帐数据包括允许减少在所述公钥加密设备和所述私钥解密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,将对帐函数应用于所述第一原始共享密钥和所述对帐数据的至少部分,并且

对经掩蔽的传输密钥(c)进行解掩蔽以获得近码字,并且根据纠错码来应用纠错。

22. 根据权利要求15和16中的任一项所述的密码系统,其中,

所述私钥解密设备的处理器被配置为:从所述私钥解密设备接收经加密的消息,至少基于所述传输密钥来导出最终密钥,并且利用所述最终密钥对经加密的消息进行解密。

23. 根据权利要求15和16中的任一项所述的密码系统,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矩阵(b)。

24. 根据权利要求15和16中的任一项所述的密码系统,其中,

所述私钥解密设备的处理器被配置为:从所述公钥加密设备接收帮助者数据,并且应用所述帮助者数据以降低在所述私钥解密设备处获得所述传输密钥时的错误率。

25. 根据权利要求21所述的密码系统,其中,

所述第一原始密钥是矩阵,对经掩蔽的传输密钥进行解掩蔽包括:丢弃第一原始密钥矩阵的元素的至少部分的零或更多个最低有效位;从经封装的数据中减去所述第一原始密钥矩阵的元素的至少部分;并且对减法结果进行舍入。

26. 根据权利要求15和16中的任一项所述的密码系统,其中,

所述私钥解密设备的处理器被配置为:根据所述传输密钥来重建所述第二私钥矩阵,并且验证对所述第二公钥矩阵的计算和/或对经封装的传输密钥的计算。

27. 根据权利要求15和16中的任一项所述的密码系统,其中,

所述私钥解密设备的处理器被配置为:将所述第一公钥矩阵存放在公钥数据库中。

28. 根据权利要求21所述的密码系统,其中,

所述第一公钥矩阵和所述第二公钥矩阵、所述第一私钥矩阵和所述第二私钥矩阵以及所述第一原始密钥和所述第二原始密钥是有限域或环上的矩阵。

29. 一种公钥加密方法(400),包括在加密阶段期间配置第二公钥矩阵(u)的第二维度($\bar{m}$),所述公钥加密方法包括:

与私钥解密设备建立(410)通信;

获得(420)与所述私钥解密设备相关联的第一公钥矩阵(b);

获得传输密钥(K)的密钥大小,

根据所述密钥大小来生成(430)所述传输密钥(K),

通过相应地选择第二私钥矩阵(s)的第二维度($\bar{m}$)的值来确定第二私钥矩阵(s)的矩阵大小以应对所述密钥大小的所述传输密钥的掩蔽,所述第二私钥矩阵(s)的第二维度($\bar{m}$)等于所述第二公钥矩阵(u)的第二维度($\bar{m}$),

根据所述矩阵大小来生成(440)所述第二私钥矩阵(s),并且根据所述第二私钥矩阵(s)来计算第二公钥矩阵(u),

根据所述第二私钥矩阵(s)和所述第一公钥矩阵(b)来计算(450)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矩阵(s)与所述第一公钥矩阵(b)之间的矩阵相乘,

利用所述第二原始共享密钥的至少部分来掩蔽(460)所述传输密钥(K),

将对所述密钥大小和/或所述矩阵大小的指示、所述第二公钥矩阵(u)以及经掩蔽的传

输密钥传送(470)到所述私钥解密设备。

30.一种包括根据权利要求29所述的公钥加密方法(400)和私钥解密方法(500)的密码方法,所述私钥解密方法(500)包括:

与公钥加密设备建立(510)通信,

生成(520)第一私钥矩阵(r),并且根据所述第一私钥矩阵(r)来计算第一公钥矩阵(b),并且允许将所述第一公钥矩阵(b)传送到所述公钥加密设备,

从所述公钥加密设备接收(530)对密钥大小和/或矩阵大小的指示、第二公钥矩阵(u)和经掩蔽的传输密钥(c),其中,在加密阶段期间,在所述公钥加密设备处,所述第二公钥矩阵(u)的第二维度($\bar{m}$)是能配置的,

根据所述第二公钥矩阵(u)和所述第一私钥矩阵(r)来计算(540)第一原始共享密钥(k'),计算所述第一原始共享密钥包括所述第二公钥矩阵(u)与所述第一私钥矩阵(r)之间的矩阵相乘,

使用所述第一原始共享密钥(k')的至少部分,根据接收到的大小对经掩蔽的传输密钥(c)进行解掩蔽(550)以获得传输密钥。

31.一种瞬态或非瞬态计算机可读介质(1000),其包括表示使处理器系统执行根据权利要求29或30所述的方法的指令的数据(1020)。

具有减小的公钥大小的公钥/私钥系统

技术领域

[0001] 本发明涉及公钥加密设备、私钥解密设备、公钥加密方法、私钥解密方法和计算机可读介质。

背景技术

[0002] 解决密钥分配问题的一种方法是使用所谓的非对称密码术。在非对称密码术中，使用包括公钥和私钥的密钥对。因此，非对称密码术也被称为公钥密码术。

[0003] 公钥可以被广泛地传播，但是私钥通常只有很少的参与方知道，例如，只有其所有者才知道。公钥能够用于对只能用私钥解密的消息进行加密。在公钥加密系统中，任何人都能够使用接收者的公钥对消息进行加密。只能使用接收者的私钥对加密的消息进行解密。根据私钥的对应公钥寻找私钥在计算上是不切实际的。公钥和私钥被称为密钥对。

[0004] 已知的公钥加密系统依赖于基于数学问题的密码算法，该数学问题目前尚无有效的解。例如，RSA公钥加密系统依赖于整数分解的难度。基于椭圆曲线的公钥加密依赖于离散对数的难度。

[0005] 量子计算机对现代密码学构成了重大威胁。通用量子计算机将破坏两种最广泛采用的公钥密码系统，即，RSA和椭圆曲线密码术(ECC)。基于格点的密码术可以用作对抗量子计算机的替代方案。不幸的是，格点计算需要大型公钥来确保其安全性。

[0006] Joppe Bos等人的“Frodo:Take off the ring!Practical,Quantum-Secure Key Exchange from LWE”(国际密码学研究协会,第20170227:170204卷,2017年2月27日,第1-26页)公开了一种安全、实用的密钥交换协议的开发结果,该协议能够用于在预期量子对手的情况下保护互联网流量的安全。在该文章中开发的密钥交换协议被称为“Frodo”,它结合了能有效采样的噪声分布以及对公共参数的高效和动态生成,其中,LWE公共矩阵A是针对每一个密钥交换根据小随机种子生成的。

[0007] 欧洲专利申请EP 3364596 A1(皇家飞利浦公司)公开了一种被配置用于密钥交换(KEX)协议的第一电子网络节点。该第一网络节点被配置为:获得与第二网络节点共享的共享矩阵(A),该共享矩阵A中的条目是以对第一模量 q 取模来选择的;生成私钥矩阵(SI),私钥矩阵中的条目的绝对值是通过(一个或多个)边界来界定的;通过计算共享矩阵(A)与对第一模量 q 取模的私钥矩阵(SI)之间的矩阵乘积并将矩阵乘积中的条目缩小到第二模量(p)来生成公钥矩阵(P I)。

发明内容

[0008] 这些问题和其他问题通过本文描述的实施例来解决。提供了公钥加密设备和私钥解密设备。通过使用公钥加密设备,能够将传输密钥传送到私钥解密设备。传输密钥可以用于对消息进行加密。因此,有权访问公钥允许对消息进行加密,但是对所述加密的消息进行解密需要访问私钥。

[0009] 公钥加密设备可以被配置为:获得与私钥解密设备相关联的第一公钥矩阵,并且

生成第二公钥矩阵,第二公钥矩阵具有比第一公钥矩阵少的矩阵元素。

[0010] 因为第二公钥矩阵具有比第一公钥矩阵少的矩阵元素,所以减少了在加密阶段期间(例如当对消息进行加密时)的开销(例如,发送传输密钥所需的开销),特别是相对于注册阶段(例如其中通过公钥加密设备获得第一公钥)。特别地,可以以与传送第二公钥不同的方式来获得第一公钥;特别地,第一公钥可以例如与软件一起(例如与浏览器软件一起)被预先分配。这是特别有利的,因为与需要公钥加密时相比,在预先分配期间更容易获得带宽。

[0011] 各种实施例能够用于各种目标。作为第一示例,可以例如在互联网上使用临时密钥交换。实施例可以用于使总带宽开销(例如,(公钥+密文))最小化。请注意,公钥可能已经可用或者尚不可用这一事实会严重影响该等式。作为另一示例,可以使密文最小化,以例如用于诸如电子邮件之类的消息传递应用中。即使使密文的大小最小化将暗示公钥更长,这也不重要,因为只要将公钥发送一次。

[0012] 在传送传输密钥之前,这两个设备会就使用哪个公钥进行协商。例如,如果密钥是预先分配的,则公钥加密设备可能更喜欢使用预先分配的密钥。例如,如果没有预先分配公钥,则公钥加密设备可能更喜欢获得较小的公钥。如果有两个公钥可用,则公钥加密设备可能更喜欢较大的密钥,因为这样可以减小传送经加密的消息所需的带宽。

[0013] 有趣的是,可以在加密时(例如在加密阶段期间)而不是在例如注册阶段期间决定第二公钥的大小。这样做的优点是,可以根据要与第二公钥一起传送的传输密钥的大小来选择第二公钥的大小。例如,对于高安全性应用程序,传输密钥可能比较低安全性应用程序具有更多的位。在后一种情况下,传送传输密钥的开销可能较小。

[0014] 在实施例中,第二公钥矩阵具有第一系统维度和第二维度,第一公钥矩阵具有第一系统维度和第二维度,第二公钥矩阵的第二维度小于第一公钥矩阵的第二维度。特别地,第二公钥矩阵的第二维度可以是1;第一公钥的第二维度可以大于1。

[0015] 在实施例中,将高噪声格点问题与奇偶校验位组合以获得小于1.5kB的第二公钥,由此当在计算机网络中使用这样的实施例时避免了数据包分片。

[0016] 公钥加密(PKE)可以基于非结构化的格点问题,例如,如在有错误的学习中或在具有舍入问题的学习中或在其组合中就是如此。实施例可以被优化以确保解密器产生最小的带宽和计算开销,但是这会以解密器需要更大的公钥为代价。尽管如此,仅需要对公钥通信一次并进行存储即可。不仅可以减小加密所需的带宽,而且还可以提高加密效率,因为加密速度会更快并且使得密码文本更小。具体来说,非环形配置的密文可以小于2000B。

[0017] 公钥加密设备和私钥解密设备可以是电子设备。例如,它们可以是计算机或服务器等。它们可以是移动电子设备,例如,移动电话、智能卡。公钥加密设备和私钥解密设备可以是消费电子设备,例如,机顶盒、电视机。公钥加密设备可以是传感器。

[0018] 根据实施例的设备和方法可以被广泛应用于实际应用中。这样的实际应用包括许多密码协议。这样的实际应用包括消息传递应用、传感器网络、数据通信、金融应用等。

[0019] 该方法的实施例可以作为计算机实施的方法在计算机上实施,或者在专用硬件中实施,或者在这两者的组合中实施。用于方法的实施例的可执行代码可以被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、光学存储设备、集成电路、服务器、在线软件等。优选地,计算机程序产品包括被存储在计算机可读介质上的非瞬态程序代码,该

非瞬态程序代码用于当所述程序产品在计算机上被执行时执行该方法的实施例。

[0020] 在实施例中,计算机程序包括计算机程序代码,该计算机程序代码适于当计算机程序在计算机上运行时执行该方法的实施例的全部或部分步骤。优选地,计算机程序被体现在计算机可读介质上。

[0021] 本发明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商店、Google的Play商店或Microsoft的Windows商店并且可从此类商店下载该计算机程序时,将使用这方面。

附图说明

[0022] 将仅通过举例的方式并参考附图来描述本发明的进一步的细节、方面和实施例。为了简单和清楚地图示附图中的元件,这些元件并不一定是按比例绘制的。在附图中,与已经描述的元件相对应的元件可以具有相同的附图标记。在附图中:

[0023] 图1a示意性地示出了私钥解密设备100的实施例的示例,

[0024] 图1b示意性地示出了公钥加密设备200的实施例的示例,

[0025] 图1c示意性地示出了密码系统101的实施例的示例,

[0026] 图2a示意性地示出了公钥加密和私钥解密的示例,

[0027] 图2b示意性地示出了公钥加密和私钥解密的示例,

[0028] 图2c示意性地示出了握手的示例,

[0029] 图3示意性地示出了公钥加密和私钥解密的示例,

[0030] 图4示意性地示出了公钥加密和私钥解密的示例,

[0031] 图5示意性地示出了根据实施例的密码系统的示例,

[0032] 图6a示意性地示出了根据实施例的公钥加密方法的示例,

[0033] 图6b示意性地示出了根据实施例的私钥解密方法的示例,

[0034] 图7a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,

[0035] 图7b示意性地示出了根据实施例的处理器系统的表示。

[0036] 附图标记列表1a-5、7a-7b:

[0037] 10 私钥解密设备

[0038] 20 公钥加密设备

[0039] 31 注册阶段

[0040] 32 加密阶段

[0041] 33 解密阶段

[0042] 11-16 消息

[0043] 100 私钥解密设备

[0044] 130 通信接口

[0045] 191 计算机网络

[0046] 192 存储接口

[0047] 194 处理器

[0048] 196 存储器

[0049]	200	公钥加密设备
[0050]	230	通信接口
[0051]	292	存储接口
[0052]	294	处理器
[0053]	296	存储器
[0054]	300	私钥解密设备
[0055]	301	密码系统
[0056]	302	公钥存储库
[0057]	305	通信接口
[0058]	315	公钥/私钥生成器
[0059]	320	错误校正器
[0060]	325	Diffie-Hellman单元
[0061]	335	对帐单元
[0062]	340	解封装单元
[0063]	350	公钥加密设备
[0064]	355	通信接口
[0065]	360	公钥获得者
[0066]	365	公钥/专钥生成器
[0067]	370	码字生成器
[0068]	375	Diffie-Hellman单元
[0069]	380	可靠位生成器
[0070]	385	对帐数据生成器
[0071]	390	封装单元
[0072]	1000	计算机可读介质
[0073]	1010	可写部分
[0074]	1020	计算机程序
[0075]	1110	(一个或多个)集成电路
[0076]	1120	处理单元
[0077]	1122	存储器
[0078]	1124	专用集成电路
[0079]	1126	通信元件
[0080]	1130	互连
[0081]	1140	处理器系统

具体实施方式

[0082] 虽然本发明可以有許多不同形式的实施例,但是在附图中示出且将在本文中详细描述一个或多个特定实施例,应当理解,本公开内容被认为是本发明原理的示例,并非旨在将本发明限于所示和所述的特定实施例。

[0083] 在下文中,为了便于理解,在操作中描述了实施例的元件。然而,很明显,各个元件

被布置为执行由它们执行的所述功能。

[0084] 另外,本发明不限于这些实施例,并且本发明在于本文描述的或在互不相同的从属权利要求中记载的每个新颖特征或特征组合。

[0085] 图1a示意性地示出了私钥解密设备100的实施例的示例。图1b示意性地示出了公钥加密设备200的实施例的示例。私钥解密设备也可以被称为第一设备或第一密码设备。公钥加密设备也可以被称为第二设备或第二密码设备。图1c示意性地示出了密码系统101的实施例的示例,该密码系统101包括私钥解密设备100和公钥加密设备200。私钥解密设备100和公钥加密设备200可以分别包括以下各项中的一项或多项:存储接口192、292,处理器194、294和存储器196、296。私钥解密设备100被配置为生成公钥/私钥对。公钥和私钥分别包括公钥矩阵和私钥矩阵。公钥加密设备200被配置为使用公钥矩阵并且使用它来使得传输密钥能够被传送到私钥解密设备。例如,传输密钥可以用作密钥,通常用作对称密钥,以对消息进行加密和稍后对消息进行解密,该消息将从公钥加密设备被传送到私钥解密设备。私钥解密设备被配置为使用私钥矩阵来获得相同的传输密钥。替代地,传输密钥可以用作针对另外的密钥协商的输入,例如,传输密钥可以与一个或多个另外的密钥输入组合,以例如导出最终密钥,例如通过使用采用传输密钥和另外的密钥输入的密钥推导函数来导出最终密钥。所述另外的密钥输入可以包括从协议获得的导出的另外的传输密钥,在所述协议中,公钥加密设备和私钥解密设备改变位置,从而在本文中描述的各种协议中扮演相反的角色。

[0086] 私钥解密设备100和公钥加密设备200(例如,系统101的各种设备)可以通过计算机网络191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191可以是互联网。该计算机网络可以是全部或部分有线的和/或全部或部分无线的。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。这些设备包括连接接口,该连接接口被布置为根据需要进行与系统101的其他设备通信。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,私钥解密设备100和公钥加密设备200可以分别包括通信接口130、230。计算机网络191可以包括其他元件,例如,路由器、集线器等。

[0087] 可以在处理器(例如,处理器电路)中实施对私钥解密设备100和公钥加密设备200的执行,在本文中示出了其示例。私钥解密设备100(特别是私钥解密设备100的处理器)可以实施如图2a-2c、图3和图4所示的私钥解密设备10的功能。公钥加密设备200(特别是公钥加密设备200的处理器)可以实施这些附图中的公钥加密设备20的功能。例如,这些功能可以全部或部分地在设备100或200处存储的计算机指令来实施,例如以在设备的电子存储器中存储的计算机指令来实施,并且能由设备的微处理器来执行。在混合式实施例中,功能单元部分地以硬件(例如作为协处理器,例如,密码协处理器)来实施,并且部分地以在设备100或200上存储和执行的软件来实施。

[0088] 设备100和200可以包括用于存储和/或检索消息(可能是加密的消息)的存储接口。例如,存储接口可以在本地实施,例如,作为去往在设备中包括的存储器(例如,分别为存储器196或296)的接口来实施。存储接口还可以与离线的(例如非本地的)存储装置(例如,云存储装置)接口连接,例如与位于另一设备中的诸如存储器或驱动器之类的存储装置接口连接。如果使用云存储装置,则设备也可以包括本地存储装置,例如,存储器。例如,存

储器可以用于存储计算机编程指令,临时存储文件等。

[0089] 在设备100和200的各种实施例中,可以从各种替代方案中选择通信接口。例如,该接口可以是去往局域网或广域网(例如,互联网)的网络接口、去往内部或外部数据存储装置的存储接口、应用程序接口(API)等。在实施例中,在同一设备中实施密钥加密设备和私钥解密设备。这对消息的加密和解密都会有帮助。例如,通信接口可以是存储接口,在这种情况下,该设备可以用于以加密形式存储消息并随后对消息进行检索和解密。

[0090] 设备100和200可以具有用户接口,该用户接口可以包括诸如一个或多个按钮、键盘、显示器、触摸屏等的公知元件。该用户接口可以被布置用于适应于发起密钥协商协议,响应密钥协商协议,发送利用公钥加密的消息,利用公钥对消息进行解密等的用户交互。

[0091] 存储装置可以被实施为电子存储器(例如,闪速存储器)或磁性存储器(例如,硬盘)等。存储装置可以包括多个分立的存储器,它们一起构成存储装置。存储装置也可以是临时存储器,例如,RAM。

[0092] 通常,设备100和200各自包括微处理器,该微处理器执行在设备100和200处存储的适当软件;例如,该软件可能已经被下载和/或被存储在对应的存储器(例如,诸如RAM之类的易失性存储器或诸如闪速存储器之类的非易失性存储器)中。替代地,设备100和200可以全部或部分地以可编程逻辑单元来实施,例如被实施为现场可编程门阵列(FPGA)。设备100和200可以全部或部分地被实施为所谓的专用集成电路(ASIC),例如,针对其特定用途而定制的集成电路(IC)。例如,可以例如使用诸如Verilog、VHDL等的硬件描述语言在CMOS中实施该电路。

[0093] 在实施例中,设备100和200可以包括一个或多个电路以实施相应设备的一种或多种或所有功能。电路可以实施本文描述的对应功能。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方式表示的指令。

[0094] 处理器电路可以以分布式方式来实施,例如被实施为多个子处理器电路。存储装置可以被分布在多个分布式子存储装置上。存储器的部分或全部可以是电子存储器、磁性存储器等。例如,存储装置可以具有易失性部分和非易失性部分。存储装置的部分可以是只读的。电路也可以是FPGA、ASIC等。

[0095] 图2a示意性地示出了公钥加密和私钥解密的示例。公钥加密侧由公钥加密设备20来执行。私钥解密侧由私钥解密设备10来执行。如上所述,图1a-4的协议可以由公钥加密设备200和私钥解密设备100来执行。

[0096] 图2a-4中的符号如下:

[0097] • a 表示公共矩阵,例如,具有在整数或环、场等中的元素的矩阵。元素可以是对模量(例如,2的幂)取模的整数。元素可以是对模量(例如,2的幂)和多项式取模的多项式。矩阵 a 通常是正方形 $d \times d$ 矩阵。对模量取模的矩阵被称为无环配置。具有对多项式和模量取模的多项式条目的矩阵被称为模块配置。

[0098] • r 和 s 分别表示私钥解密设备和公钥加密设备的私钥矩阵。

[0099] • b 和 u 表示私钥解密设备和公钥加密设备的公钥矩阵, b 和 u 被图示为乘积 $a*r$ 或乘积 $a*s$ 。

[0100] 运算 $*$ 表示基础问题的单向函数。星号($*$)运算会根据两个基础矩阵来导出新的数

学对象(例如,新的矩阵),同时会引入一些噪声。例如,可以通过加上噪声元素来显式地引入噪声,或者例如通过舍入来隐式地引入噪声。能够在(R)LWE或(R)LWR或它们的模块版本中找到星号运算的示例。例如, $a*r$ 可以表示 $((A*r \pmod{q}), p, q)$,例如在LWR中的情况。这意味着 r 乘以对 q 取模的平方矩阵 A 的乘积。然后,通过执行 $p/q (A*r \pmod{q})$ 来用整数 p 和 q 对结果进行舍入,其中, $p < q$ 。

[0101] • c 表示经封装的传输密钥 K

[0102] • $\text{encapsulate}(k, K)$ 表示用 k 对传输密钥 K 进行封装。例如,如果 k 在 Z_q 中,那么也可以在 Z_q 中表示 K 。如果 k 在 Z_2 中,那么这可能是XOR。可以逐元素进行封装,例如将 k 和 K 解读为如下矩阵:

[0103] $c = k + K * (q/2) \pmod{q}$ 。

[0104] 例如,封装函数可以使用密钥 k 来掩蔽传输密钥 K ,使得 k 中的错误对 m 具有有限的影响(例如,线性影响)。例如,例如通过将 K 中的元素乘以 Z_q 中的元素可以将传输密钥 K 中的位映射到 Z_q ;如果 q 为偶数,则 $q/2$ 是个好选择。接下来,将密钥 k 的元素(其也可能是 Z_q 的元素)加上 K 的映射元素。

[0105] • $\text{decapsulate}(k, c)$ 表示使用返回位串的密钥 k 对密文 c 进行解封装。

[0106] 参考文献:

[0107] RLWE:Vadim Lyubashevsky,Chris Peikert和Oded Regev撰写的“论理想的格点和环上有错误的学习(On Ideal Lattices and Learning with Errors Over Rings)”,

[0108] RLWR:Abhishek Banerjee,Chris Peikert和Alon Rosen撰写的“伪随机函数和格点(Pseudorandom Functions and Lattices)”,

[0109] LWE:Oded Regev撰写的“论格点、有错误的学习、随机线性代码和密码术(On Lattices, Learning with Errors, Random Linear Codes, and Cryptography)”。

[0110] LWR:Abhishek Banerjee,Chris Peikert和Alon Rosen撰写的“伪随机函数和格点(Pseudorandom Functions and Lattices)”,

[0111] HILA5:Markku-Juhani O.Saarinen撰写的“HILA5:论环-LWE加密的可靠性、对帐和纠错(On Reliability, Reconciliation, and Error Correction for Ring-LWE Encryption)”。

[0112] 星号运算可以是噪声矩阵相乘,例如,规则矩阵相乘,然后加上噪声。加上噪声也可以与矩阵相乘集成在一起。在星号运算中加上噪声可以通过多种方式来完成。加上噪声的一个示例是加上显式噪声(例如生成并加上噪声矩阵)。加上显式噪声的优点是,该噪声在密码学家的完全控制下,并且能够进行精细调谐,以例如获得对系统失败率相对于系统安全性的精确控制。此外,加上显式噪声的优点是,所有矩阵都在同一环或场等上,由此简化了分析。加上噪声的另一示例是缩小比例。例如,矩阵 a 、 r 和 s 可以具有对模量 q 取模的元素(例如,对 q 取模的整数或多项式);例如通过与 p/q 相乘并进行舍入(例如,向上舍入或向下舍入或舍入到最接近的整数等),星号运算可以将矩阵运算的结果从对 q 取模向下舍入到对 p 取模。

[0113] 在本申请中,将使用小写字母表示矩阵,但应当理解,在任何需要的地方(例如根据矩阵的维度的要求以及两侧的原始密钥应大致相等的要求)可能需要对矩阵进行转置。通常,有一种以上的方法可以做到这一点。例如,通过在实施例中转置所有矩阵,可以获得

替代的工作实施例。

[0114] 下面给出了一个示例,其中,矩阵对象以大写字母给出,并且其中包括转置。秘密密钥被定义为矩阵 $S \in \mathbb{Z}^{d \times \bar{n}}$ 和 $R \in \mathbb{Z}^{d \times \bar{m}}$ 。请注意,这样的秘密密钥矩阵实际上包含分别为 $\bar{n}$ 和 $\bar{m}$ 个的独立的秘密密钥向量。原始密钥矩阵等于 $S^T A^T R$ 且在 $\mathbb{Z}^{\bar{n} \times \bar{m}}$ 中。从原始密钥的条目中的每个中,提取出 B 个最高有效位,使得能够生成长度为 $\bar{n} * \bar{m} * B$ 的总原始密钥。之所以这样称呼原始密钥,是因为存在在公钥加密设备和私钥解密设备处导出的原始密钥不完全相等的概率。

[0115] 在注册阶段31中:

[0116] 私钥解密设备选择公共矩阵 A 和第一私钥矩阵 R

[0117] 私钥解密设备为某些错误矩阵 E 计算第一公钥矩阵 $B = AR + E$

[0118] 私钥解密设备发送: A 、 B

[0119] 在加密阶段32中:

[0120] 公钥加密设备选择第二私钥矩阵: S

[0121] 公钥加密设备为某些错误矩阵 E' 计算第二公钥矩阵: $U = A^T S + E'$

[0122] 公钥加密设备计算第二原始密钥 $B^T S$, 请注意, $B^T S = S^T A^T R + E'^T R$

[0123] 公钥加密设备生成传输密钥 K , 并且将经封装的传输密钥与对帐数据一起计算为

$$C = \left(\frac{p}{2^B}\right) K + B^T R$$

[0124] 公钥加密设备发送: U 、 C

[0125] 在解密阶段33中:

[0126] 私钥解密设备计算第一原始密钥 $S^T U$, 请注意, $S^T U = S^T A^T R + S^T E'$

[0127] 私钥解密设备通过计算 $C - S^T U$ 来进行解封装, 并且将结果舍入为 $\left(\frac{p}{2^B}\right)$ 的倍数。接下来,

可以例如通过除以 $\left(\frac{p}{2^B}\right)$ 来根据舍入获得传输密钥 K

[0128] 在上面的示例中, 矩阵 A 、 B 、 S 、 U 和 R 在 $\mathbb{Z}_p$ 上。指数 2^B 中的值 B 指示取自原始密钥的用于封装 K 的最高有效位的数量。在该示例中, 其余的较低有效位用作对帐数据。例如, 可以取 $B=4$ 个位来用于封装。例如, 模量可以被选择为 $p=2^{12}$ 。传输密钥可以被编码为矩阵, 其中的条目在 $\mathbb{Z}_{2^B}$ 中, 例如, 其中的条目选自 $\{0, 1, \dots, 2^B - 1\}$ 。矩阵 E 和 E' 可以是其条目是对 p 取小模的矩阵。例如, 它们可以选自以下集合:

[0129] $\{0, 1, \dots, w-1\} \cup p - (w-1), p - (w-1) + 1, \dots, p-1$

[0130] 其中具有小的 w 。 w 的大小被选择为平衡系统安全性与系统失败率。 w 的值较低会降低系统失败率。

[0131] 矩阵 C 可以被计算为对 p 取模。出于带宽效率的原因, 公钥加密设备可以在 t 除以 p 的情况下计算并发送 $C = \left(\frac{t}{2^B}\right) M + B^T R \bmod t$ 。在恢复 M 时, 私钥解密设备计算

$\left(\frac{p}{t}\right) C - S^T U \bmod p$ 。在这种情况下, 原始密钥的用作对帐数据的位数少于可用位数。通常, 较低有效位对失败概率的影响较小。

[0132] 代替使用错误矩阵,可以将示例修改为在星号运算中按比例缩小以加上噪声,而不是加上显式噪声。按比例缩小具有减小带宽的优点。

[0133] 返回图2a。示出了注册阶段31,其中,私钥解密设备10生成其私钥矩阵和公钥矩阵,并且使公钥可用于公钥加密设备20。例如,可以将公钥发送到设备20。例如,公钥可以被存放在公钥数据库中,设备20可以从该公钥数据库中检索公钥。例如,设备10和20可以是不同的设备,也可以是相同的设备。

[0134] 在注册阶段31期间,设备10生成第一私钥矩阵(r),并且根据第一私钥矩阵(r)来计算第一公钥矩阵(b)。例如,设备10可以生成公共矩阵(a),并且将第一公钥矩阵(b)计算为第一私钥矩阵(r)与公共矩阵(a)之间的噪声矩阵相乘。布置第一公钥矩阵(b)从私钥解密设备到公钥加密设备20的传送。例如,可以在消息11中将第一公钥矩阵(b)从私钥解密设备发送到设备20。

[0135] 公共矩阵(a)在公钥加密设备与私钥解密设备之间共享,第一公钥矩阵(b)与公共矩阵(a)相关联。例如,以与公钥矩阵(b)相同的方式将公共矩阵传送到设备20。通常,将根据种子来伪随机生成矩阵 a 。能够通过发送种子来共享该矩阵。

[0136] 加密阶段32可以晚于注册阶段31,甚至比其晚得多。在加密阶段32中,设备20生成传输密钥(K),生成第二私钥矩阵(s),并且根据第二私钥矩阵(s)来计算第二公钥矩阵(u)。例如,设备20可以获得与第一公钥矩阵(b)相关联的公共矩阵(a),并且将第二公钥矩阵(u)计算为第二私钥矩阵与公共矩阵(a)之间的噪声矩阵相乘。可以以据其生成公共矩阵的种子的形式获得公共矩阵。在实施例中,公共矩阵是从不同的源获得的。例如,设备10和设备20都可以从第三方获得公共矩阵。

[0137] 生成传输密钥可以随机进行。

[0138] 设备20被配置为:根据第二私钥矩阵(s)和第一公钥矩阵(b)来计算第二原始共享密钥(k^*),计算第二原始共享密钥包括第二私钥矩阵(s)与第一公钥矩阵(b)之间的矩阵相乘;通过应用封装函数,利用第二原始共享密钥的至少部分来封装传输密钥(K),从而获得经封装的数据(c);并且将第二公钥矩阵(u)和经封装的数据(c)传送到私钥解密设备。例如,可以在消息12中将第二公钥矩阵(u)和经封装的数据(c)发送到私钥解密设备。

[0139] 请注意,这允许传输密钥与原始密钥无关。这样可以增强抵御主动攻击的能力。

[0140] 在私钥解密设备从公钥加密设备接收到第二公钥矩阵(u)和经封装的数据(c)之后,私钥解密设备能够在解密阶段33中继续进行以根据第二公钥矩阵(u)和第一私钥矩阵(r)来计算第一原始共享密钥(k'),计算第一原始共享密钥包括第二公钥矩阵(u)与第一私钥矩阵(r)之间的矩阵相乘,并且使用第一原始共享密钥(k')的至少部分对经封装的数据(c)进行解封装以获得传输密钥。

[0141] 有趣的是,在实施例中,第二公钥矩阵(u)具有比第一公钥矩阵(b)少的矩阵元素。如果所有矩阵都是正方形的并且维数相同,则第二公钥矩阵(u)和第一公钥矩阵(b)将具有相同数量的元素。发明人的见解是,这是不需要的。这继而意味着公钥对消息11和12的贡献将是相等的。然而,发送这些消息的环境和发送消息的设备可能会大不相同。通过将第二公钥矩阵(u)的大小选择为小于第一公钥矩阵(b)的大小,消息12的带宽需求会减少,而消息11的带宽需求会增加。

[0142] 可以使第二公钥矩阵(u)的大小小于第一公钥矩阵(b)的矩阵元素的数量的一种

方式是选择适当较小的第二私钥矩阵。特别地,第二私钥矩阵(s)可以被选择为具有比第一公钥矩阵(b)少的矩阵元素。这可能意味着第二公钥矩阵(u)也具有比第一私钥矩阵(r)少的矩阵元素。

[0143] 例如,在实施例,选择系统维度(d)。系统维度部分决定了系统的安全性。 n 的值越高,对应的安全性就越高。矩阵a、r、b、s、u中的每个的多个维度之一等于系统维度d。如果使用错误矩阵,则错误矩阵e、e'也由有一个维度等于系统维度。如果原始密钥k、k'和/或传输密钥K被表示为矩阵,则它们也有一个维度等于系统维度。可以选择这些矩阵的其他维度,使得能够兼容相加和相乘(可能包括转置)。

[0144] 在实施例,公共矩阵a是维度 $d \times d$ 的正方形矩阵。第一私钥矩阵r和第一公钥矩阵b具有维度 $d \times \bar{n}$ 。第二私钥矩阵s和第二公钥矩阵u具有维度 $d \times \bar{m}$ 。通过将第二私钥矩阵s和第二公钥矩阵u的第二维度 $\bar{m}$ 选择为小于第一私钥矩阵r和第一公钥矩阵b的第二维度 $\bar{n}$,确保了消息12中的公钥u的条目少于消息11中的公钥b的条目。

[0145] 例如,通过将第二公钥矩阵(u)的第二维度($\bar{m}$)选择为例如最多为第一公钥矩阵(b)的第二维度($\bar{n}$)的一半,确保了第二公钥矩阵(u)的条目数量最多为第一公钥矩阵(b)的条目数量的一半。

[0146] 对第二私钥矩阵和第二公钥矩阵的第二维度($\bar{m}$)的特别有利的选择是一。这使第二消息12的大小最小化。

[0147] 例如,可以在注册阶段期间发送消息11,在该注册阶段中可以使用更多的带宽。例如,可以在可用带宽较小的系统的主动参与期间发送消息12。例如,设备12可以是传感器,当有足够的带宽时(例如在生产或设置期间),该传感器被提供有第一公钥,而在传感器的使用期间(在此期间带宽较小)可以发送消息12。请注意,代替通过例如计算机网络来发送消息11,可以通过例如将第一公钥安装在设备20的存储器设备上在设备20处获得第一公钥。

[0148] 有趣的是,系统的安全性被认为更多地取决于系统维度d和乘积 $B\bar{n}\bar{m}$,而不是取决于 $\bar{n}$ 和 $\bar{m}$ 的个体尺寸。后者指示能够用于导出原始密钥的长度(以位为单位)。前者影响基础格点的大小,由此影响基础密码问题的难解度。该方案解密失败的概率部分取决于B的值。较高的B值会加重失败率并对PKE方案抵御自适应主动攻击的安全性产生不利影响。通常,B是固定的,例如为标准化参数集的形式。

[0149] 因此,通过在减小 $\bar{m}$ 的大小的同时增加第一公钥的大小(例如, $\bar{n}$ 的大小),能够在减小消息12所需的带宽的同时保持相同的安全性。特别地,其中 $\bar{n} = d$ 且 $\bar{m} = d$ 的系统与其中 $\bar{n} = d^2$ 且 $\bar{m} = 1$ 的系统具有可以相提并论的安全性。

[0150] 有趣的是,不需要预先确定第二公钥矩阵(u)的第二维度($\bar{m}$)。能够独立于对第一私钥和公钥所做的选择来选择它。特别地,可以独立于维度($\bar{n}$)来选择它。在实施例,在第二设备20处能够配置第二维度($\bar{m}$)。

[0151] 在示例实施例,可以使用 $B=4$, $\bar{n} = 64$, $\bar{m} = 1$ 。B指示原始密钥矩阵条目使用的最高有效位数。

[0152]	长期公钥配置	
	d、n	1198、1
	q、p、t	2^{14} 、 2^{12} 、 2^{10}
	B、 $\bar{n}$ 、 $\bar{m}$	4、64、1
	μ	64

[0153] 在上表中：

[0154] n指示私有矩阵和/或公共矩阵中多项式的阶数。值 $n=1$ 指示使用对模量取模的整数。该值n可以被称为“环维度”，例如，所选择的多项式环的阶数。

[0155] d指示系统维度，例如，公共矩阵a的列数和行数，

[0156] μ 指示用于封装传输密钥的原始密钥矩阵的元素数。这些元素可以是预先确定的（例如是标准化的），或者可以是随机选择的，或者可以是故意的，例如作为可靠的元素等。共享秘密密钥长度因此为 μB ；在上面的示例中，这是 $64 \times 4 = 256$ 。

[0157] 在实施例中，第一公钥可以包括：

[0158] 1、用于再生公共矩阵a的种子。例如，种子的位长可以被选择为与共享秘密相同；在该示例中为256位。

[0159] 2、公钥矩阵b。该矩阵的维度可以为d和 $\bar{n}$ ，并且可以选择对p取模的元素。例如，第一秘密矩阵可以选择对q取模的元素。在这种情况下，可以通过从q向下缩放到p来加上噪声。该示例中的公钥矩阵能够按 $\log_2 p d \bar{n}$ 位进行编码；在该示例中为 $12 \times 1198 \times 64 = 920064$ 位。

[0160] 3、任选地，额外的记账信息。例如，可以包括标识符以指示密钥的类型；例如，1个字节。例如，标识符可以指示公共矩阵a的再生方法。例如，可以包括值 $\bar{n}$ （例如2个字节）。该值 $\bar{n}$ 的两个字节允许选择更大的 $\bar{n}$ 值，例如，在一些用例中， $\bar{n}$ 也可能为512的值。这些值和标识符可以例如由系统设计者来预先确定，在这种情况下，不需要包括它们。然而，包括 $\bar{n}$ 值允许从加密阶段到注册阶段动态移位带宽，例如移位到应用所需的程度。

[0161] 在该示例中，公钥矩阵的总大小为115008个字节。如果包括种子和/或标识符，则可以加上额外的32或35个字节等。请注意，可以以各种方式来生成秘密密钥。例如，私钥矩阵可以是完全随机的，但是它可能受到限制，例如受到汉明权重限制。例如，私钥矩阵中的长度为d的向量可以具有预先确定的汉明权重；例如，在该示例中，可以选择汉明重量574。

[0162] 在实施例中，密文可以包括：

[0163] 1、第二公钥矩阵u。第二公钥矩阵可以具有维度d和 $\bar{m}$ ，并且选择对p取模的元素。该示例中的公钥矩阵能够按 $\log_2 p d \bar{m}$ 位进行编码；在该示例中是 $12 \times 1198 \times 1 = 14376$ 位。

[0164] 2、经封装的数据c可以被编码为具有 μ 个元素的向量，其中选择对t取模的元素。在

该示例中,经封装的数据的大小为 $\mu \log_2 t$ 位;在该示例中是 $64 \times 10 = 640$ 位。可以认为该方案使用 $\log_2 t - B$ 对帐位;在这种情况下为6。

[0165] 3、任选地,在对消息使用经过认证的加密的情况下,认证标签。例如,如果使用Galois/计数器模式,则认证标签可以是AESGCM认证标签。不需要在PKE方案的公钥中包括认证标签。

[0166] 4、任选地, $\bar{m}$ 的值。例如,这可以是1个字节。

[0167] 因此,在该示例中,密文大小可以是 $12 \times 1198 \times 1 + 64 \times 10 = 15016$ 位,即,1877个字节。密文大小不包括经加密的消息的大小。任选地,一些位(例如,8个位)可以用于传输 $\bar{m}$ 的值。该示例的PQ安全性被估计为 2^{233} ,并且失败率被估计为 2^{-129} 。

[0168] 在实施例中,可以使用Hayo Baan等人的“Round2:KEM and PKE based on GLWR”中的更加完善的封装函数(如算法9)来进一步增强主动安全性。如果是这样,则密文可以包括散列 g ,该散列 g 可以由公钥加密设备通过对私钥解密设备的公钥进行散列化来计算。该散列可以用于确保最终共享秘密包含来自私钥解密设备和公钥加密设备这两者的贡献。例如,可以使用Fujisaki-Okamoto变换。该散列可以例如是共享秘密的大小,在该示例中为256位。

[0169] 如以上所指出的,传输密钥可以用于对消息 m 进行加密。例如,公钥加密设备可以被配置为:利用传输密钥对消息(m)进行加密,并且将所述加密的消息传送到私钥解密设备。私钥解密设备可以从公钥加密设备接收经加密的消息(例如连同第二公钥矩阵和经封装的数据),并且利用传输密钥对经加密的消息进行解密。

[0170] 在实施例中,传输密钥独立于第一公钥矩阵(b)。例如,可以在不使用第一公钥矩阵(b)的情况下生成传输密钥 K ,例如,可以随机生成传输密钥,并且/或者在设备20接收到第一公钥矩阵(b)之前生成传输密钥。

[0171] 同样,传输密钥可以独立于第一私钥矩阵(r)。传输密钥可以在计算上独立于第二私钥矩阵(s)和第二公钥矩阵(u)、经封装的数据(c)。在计算上独立意味着在攻击者的计算边界内,第二私钥矩阵的知识不会提供关于传输密钥的信息。

[0172] 传输密钥 K 通常是暂时使用的,例如它可以是临时的,例如仅用于对单个消息 m 或单个会话、协议、握手等进行加密。传输密钥 K 可以是对称密钥,例如用作分组密码中的密钥。

[0173] 例如,设备20可以被配置为在封装传输密钥之后删除对消息进行加密的传输密钥和/或第二私钥矩阵。例如,可以在将经封装的数据发送到设备10之前删除传输密钥和/或第二私钥矩阵。同样,设备10可以在对消息进行解密之后删除传输密钥。

[0174] 在实施例中,第二私钥矩阵是根据传输密钥导出的。例如,传输密钥可以是随机生成的(可以是真的也可以是伪的),然后用作针对密钥推导函数(例如,散列函数)的输入以导出种子。也可能有其他输入,例如,消息、第一公钥矩阵等。然后,将种子用于生成第二私钥矩阵,例如,作为取决于种子的确定性伪随机函数。优选地,密钥推导函数被选择为使得无法根据第二私钥矩阵计算出传输密钥。

[0175] 这具有以下效果:在设备10导出传输密钥之后,设备10能够例如通过应用相同的密钥推导函数并根据该密钥推导函数计算第二私钥矩阵来根据传输密钥重建第二私钥矩阵。接下来,设备10能够验证第二公钥和/或经封装的数据是否被正确计算。这样做的优点

是主动攻击更难完成。如果设备10发现异常,例如接收到的数据与重新计算的第二公钥和/或重新计算的经封装的数据之间存在差异,则设备10可以采取适当的措施,例如生成警告信号,中止解密第二消息等。

[0176] 根据传输密钥导出第二私钥矩阵的优点是,其安全性相对于CCA安全系统而言更高。这是有利的,特别是在一次生成第一公钥矩阵并将其用于许多消息的情况下。

[0177] 在实施例中,公钥加密设备的处理器被配置为计算帮助者数据以减少在私钥解密设备处获得传输密钥时的错误率。基于噪声矩阵相乘的公钥加密的本质是,私钥解密密钥一侧的传输密钥重建可能会失败。能够通过多种方式降低失败概率,其中一种方式是计算并发送帮助者数据以帮助私钥解密设备获得正确的传输密钥。

[0178] 例如,私钥解密设备可以被配置为:从公钥加密设备接收帮助者数据,并且应用该帮助者数据以减少在私钥解密设备处获得传输密钥时的错误率。

[0179] 可以使用若干类型的帮助者数据。在上面给出的示例中,使用了一种方法,即,对帐数据。第二原始密钥的部分可以用于封装传输密钥,并且第二原始密钥的部分可以用作对帐数据。

[0180] 例如,在实施例中,第二原始密钥是矩阵,封装传输密钥(K)包括:将传输密钥的位加到第二原始密钥矩阵的元素的至少部分的最高有效部分,并且丢弃第二原始密钥矩阵的元素的至少部分的零或更多个最低有效位。在实施例中,没有被加到传输密钥以传输密钥其进行封装的所有位都可以被用作对帐数据。然而,为了减小带宽,可以丢弃最低有效位中的一个或多个。请注意,并非必须使用原始密钥矩阵的所有矩阵元素。未使用的元素能够全部丢弃。这样可以节省带宽。在设备10处,对经封装的数据进行解封装可以包括:丢弃第一原始密钥矩阵的元素的至少部分的零或更多个最低有效位,从经封装的数据中减去第一原始密钥矩阵的元素的至少部分,然后将减法结果进行舍入。有趣的是,帮助者数据很容易被集成在经封装的传输密钥中。

[0181] 在实施例中,公钥加密设备被配置为执行以下操作中的一项或多项:

[0182] a) 将可靠的位函数应用于第二原始共享密钥(k^*),从而选择第二原始共享密钥的部分,获得指示第二原始共享密钥的元素的可靠索引(用于封装的位是根据所指示的元素导出的);并且将可靠索引传送到私钥解密设备,并且/或者

[0183] b) 生成针对第二原始共享密钥的至少部分的对帐数据(h),该对帐数据包括允许减小在公钥加密设备和私钥解密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,并且将对帐数据(h)传送到私钥解密设备,并且/或者

[0184] c) 生成针对传输密钥的奇偶校验位,传输密钥和奇偶校验位根据纠错码形成码字,封装传输密钥包括封装码字。

[0185] 同样,私钥解密设备可以被配置为执行以下操作中的一项或多项:

[0186] a) 从公钥加密设备接收可靠索引,从而选择由可靠索引指示的第一原始共享密钥的部分,

[0187] b) 接收针对第一原始共享密钥(k')的至少部分的对帐数据(h),该对帐数据包括允许减少在公钥加密设备和私钥解密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,将对帐函数应用于第一原始共享密钥和对帐数据的至少部分,并且

[0188] c) 对经封装的数据(c)进行解封装以获得近码字,并且根据纠错码来应用纠错。

[0189] 可靠位是更可能在两侧均等地计算的位。例如,原始密钥矩阵的一些元素可以被确定为可靠,而其他不可靠的元素可以被丢弃。对于所选择的矩阵元素,可以获得对帐数据。最后,可以计算奇偶校验位以计算其他错误。这三种类型的帮助者数据是独立的,因为可以使用每一种或每两种或全部三种帮助者数据来降低私钥解密的失败率。

[0190] 在实施例中,对帐数据和奇偶校验位被组合,但不是可靠位。这种方法的优点是不需要共享有关元素大小的信息。帮助者数据可以被包括在经封装的数据中,但是也可以从设备20被独立地传送到设备10。对帐数据可以方便地与经封装的传输密钥集成在一起,例如,如本文所图示的那样。在图3中图示了其中奇偶校验位和对帐数据被组合但不是可靠位的实施例的示例。

[0191] 在公钥加密设备或私钥解密设备的实施例中,可靠位是所指示的元素的一个或多个最高有效位,针对所指示的元素的对帐数据是所指示的元素的在可靠的有效位之后的一个或多个位,可以丢弃所指示的元素的一个或多个最低有效位。所指示的元素(即,可靠的元素)可以从公钥加密设备被传送到私钥解密设备,例如被传送到它们在矩阵中的位置。

[0192] 在私钥解密设备的实施例中,由可靠索引指示的原始密钥中的元素被选择并且被替换为与对应的对帐数据一致的经修改的元素。例如,经修改的元素可以使所选择的元素与经修改的元素之间的Lee距离最小化。可以将可靠位作为经修改的元素的一个或多个最高有效位来获得。

[0193] 在实施例中,确定经修改的元素,使得它们与对应的对帐数据一致,以至于它们不会被公钥加密设备丢弃。经修改的元素使所选择的元素与经修改的元素之间的Lee距离最小化。

[0194] 图2b示意性地示出了公钥加密和私钥解密的示例。在图2b中,“ind”表示对密钥大小或矩阵大小的指示。

[0195] 图2b所示的实施例建立在图2a的实施例的基础上。在注册阶段31期间,根据图2b的设备10可以与图2a的设备10相同。然而,在加密阶段32中,设备20被配置为获得传输密钥(K)的密钥大小并根据所述密钥大小来生成传输密钥(K)。例如,如果要加密的信息具有较高的安全性,则设备20可以选择256位传输密钥K,但是如果该信息具有较低的安全性,则设备20可以选择128位传输密钥K。设备20可以确定第二私钥矩阵(s)的矩阵大小,以适应对所述密钥大小的传输密钥的封装。例如,为了容纳较大的传输密钥,设备20可以选择较大的(例如成比例较大的)第二维度 $\bar{m}$ 。

[0196] 第二维度 $\bar{m}$ 可以被选择为使得 $\bar{m}\bar{n}B$ 等于传输密钥的期望位大小或者至少与传输密钥的期望位大小一样大。例如,为了支持256位而不是128位,第二维度 $\bar{m}$ 可以被选择为两倍大。例如, $\bar{m}$ 可以为2或1,使得 $\bar{m}\bar{n}B$ 等于256或128。

[0197] 取决于所选择的维度 $\bar{m}$,设备20根据矩阵大小(例如根据系统维度d和第二维度 $\bar{m}$)来生成第二私钥矩阵(s)。然后,基于较大的矩阵,设备20继续计算原始密钥并封装传输密钥,例如,如本文中所指示的那样,例如,在图2a的背景中那样。然而,设备20将对密钥大小和/或矩阵大小的指示ind传送到私钥解密设备。例如,指示ind可以是传输密钥的大小,例如256或128,或者“大”或“小”,或者是第二公-私钥矩阵的大小,例如,第二维度,例如2或1等。该指示可以是隐式的,例如通过发送更大或更小的第二公钥矩阵而是隐式的。例如,可

可以在一个或多个计算机网络包中发送第二公钥矩阵,该一个或多个计算机网络包指示该包的大小或结束等,从而隐式地指示第二公钥矩阵的大小,因此例如隐式地指示第二维度的大小。

[0198] 如果值 $\bar{m}\bar{n}B$ 大于封装所需的值,则可以选择故意更大的传输密钥,例如密钥大小等于 $\bar{m}\bar{n}B$ 。然后能够例如通过密钥推导函数、散列等根据所选择的传输密钥来计算最终传输密钥。

[0199] 设备10可以例如如本文中所指示的那样(例如如在图2a的背景中那样)继续进行。例如,设备10可以使用接收到的公钥矩阵来计算第一原始密钥并对经封装的传输密钥进行解封装。原始密钥的大小可能会取决于公钥的大小而有所不同。

[0200] 在实施例中,第一公钥与作为公钥的参数的参数 $\bar{n}$ 一起被传送,使得公钥加密设备能够确定所需的 $\bar{m}$ 值。例如,可以由公钥加密设备来计算 $\bar{m}$,使得 $B\bar{n}\bar{m} \geq Keylength$ 。例如,在实施例中,公钥包括公钥矩阵b、公钥矩阵a和维度 $\bar{n}$ 。后者可能是隐式的。换句话说,设备10将允许实现给定的安全水平的参数集发送到设备20。

[0201] 可以在各种现有协议中使用根据实施例的公钥加密。例如,实施例可以与诸如TLS、IPSec、VPN之类的协议集成在一起。例如:

[0202] TLS1.3:客户端发送client_hello。client_hello可以包括公钥矩阵。代替具有公钥,client_hello可以包括指示在哪里能够下载公钥矩阵的URL。如果服务器还没有例如缓存的公钥,则服务器可以继续下载公钥矩阵并将其存储在本地。利用公钥矩阵,服务器能够对发送到客户端的对称密钥进行加密并将其用作主密钥,根据该主密钥导出针对记录层的对称密钥。在该示例中,客户端充当私钥解密设备。

[0203] TLS1.2:在该示例中,是另一种方式。客户端可以发送请求,并且服务器发送在那里能够获得服务器公钥矩阵的URL。如果公钥尚不可用,则客户端可以下载公钥。并且一旦客户端具有公钥矩阵,它就能够继续加密例如要在记录层中使用的传输密钥。在该示例中,客户端充当公钥加密设备。

[0204] 请注意,可以预先分配公钥。例如,在浏览器中,可以预先分配一个或多个公钥矩阵(例如,多个公钥矩阵)。例如,可以利用公钥ID(例如,密钥的散列)来指示公钥,使得软件(例如,浏览器)能够验证是否通过预先分配获得了公钥。在预先分配的场景中,带宽不对称是个优点。例如,在预先分配期间,如果公钥矩阵较大,则这不是问题,但是在使用期间,消息的大小会减小。而且,在例如基于TLS的VPN中,可以在通信方中的一方或双方中预先配置公钥。

[0205] 在实施例中,设备10可以被配置为发送第一问候消息,该第一问候消息列出诸如SSL或TLS版本之类的密码信息,或者以客户端的偏好顺序、所支持的CipherSuite等列出密码信息。响应于第一问候消息,设备20可以发送第二问候消息。第二问候消息可以包含类似的详细信息。设备20还可以在第二问候消息中发送其数字证书。设备10可以验证证书。第一问候消息和/或第二问候消息可以包括公钥或对公钥的指示。在第二问候消息和/或随后的消息中,商定一个或多个传输密钥。传输密钥可以用于加密或认证设备10和20之间的后续通信。如果商定了多个传输密钥,则可以将它们组合成单个密钥,例如,可以将它们散列在一起或者进行异或运算等。

[0206] 图2c示意性地示出了握手的示例。握手可以与现有协议结合使用,也可以在现有协议外部使用。图2c示出了消息12-16,其中一些消息可以被组合成握手。特别地,可以省去消息13和16之一或两者。例如,可以省去消息15。时间朝向附图的底部前进。

[0207] 消息13是预先分配,在此期间,设备20获得与私钥解密设备10相关联的至少一个第一公钥矩阵 (b)。随后,当设备20和/或设备10想要参与握手协议时,设备20从设备10接收至少两个标识符,这些标识符指示私钥解密设备的至少两个第一公钥矩阵,这两个第一公钥矩阵具有不同的大小。例如,消息14可以是问候消息。消息13和14之间的省略号指示在握手开始之前已经发送了消息13。例如,设备20可以将其作为浏览器的部分而从公钥数据库等中获得公钥矩阵。

[0208] 设备20通过以下操作来选择至少两个第一公钥矩阵中的一个:确定公钥加密设备的密钥高速缓存是否包括这两个第一公钥矩阵中的较大者,并且如果这样,则选择这个较大的第一公钥矩阵。例如,设备20可以包括密钥高速缓存,先前获得的公钥矩阵被存储在该密钥高速缓存中。密钥高速缓存可以是浏览器的部分。

[0209] 设备20可以有各种策略来选择公钥。首先要考虑的是系统维度的大小。可以基于安全考虑来选择系统维度。下一考虑因素可以是期望的传输密钥的大小。另一考虑因素可以是将从设备20发送到设备10的结果消息12的大小。例如,在实施例中,设备20可以被配置为选择在密钥高速缓存中可用的最大密钥。

[0210] 如果期望的密钥在密钥高速缓存中不可用,并且特别是如果设备10的公钥在密钥高速缓存中都不可用,则设备20可以发送请求消息15;请求消息15请求所选择的第一公钥矩阵。

[0211] 作为响应,可以在消息16中将所请求的公钥发送到设备20。请注意,消息103和16不必一定来自设备10,而是可以从例如公钥数据库或软件数据库等中获得。

[0212] 一旦所选择的公钥可用,设备20就能够如本文所述的那样(例如通过封装传输密钥等)继续发送消息12。设备20将所选择的第一公钥矩阵的指示发送到私钥解密设备。利用所选择的第一公钥来封装传输密钥(K)。设备20可以使用关于图2b所描述的实施例,并且可以使用较大的公钥来选择性地封装较大或较小的传输密钥。

[0213] 设备10可以被相应地配置为:发送消息14,该消息14包括私钥解密设备的至少两个第一公钥矩阵的至少两个指示,这两个第一公钥矩阵具有不同的大小;并且接收消息12,消息12包括来自公钥加密设备的所选择的第一公钥矩阵的指示。

[0214] 根据图2c的实施例的优点在于,如果较大的密钥不引起额外的带宽(例如如果密钥是预先分配的),则可以使用较大的密钥。较大的密钥可以用于例如对较大的传输密钥和较小的传输密钥都进行加密。如果密钥不是预先分配的,则系统可以选择较小的公钥以减少带宽消耗。

[0215] 例如,在实施例中,选择大的公钥,使得 $B * \bar{n} * 1 \geq Keylength$, 其中,B是取自原始密钥矩阵的元素的位数,例如,B=1、2、4等。Keylength是该传输密钥的大小,例如,它的值可以是256。例如,在B=4的示例值和密钥长度为256的情况下,可以选择 $\bar{n} = 64$ 。可以选择小的公钥,使得 $B\bar{n}\bar{n} \geq Keylength$ 。利用相同的示例值,可以使用 $\bar{m} = \bar{n} = 8$ 。这种选择平衡了两个公钥之间所需的带宽。如果公钥加密设备有权访问大的密钥,则可以使

用大的密钥来使带宽最小化。如果公钥加密设备无权访问任何一个密钥,则公钥加密设备会请求较小的密钥来平衡带宽。在实施例中,大的第一公钥比小的第一公钥大至少2倍,大至少4倍或者大至少8倍等。

[0216] 例如,公钥加密设备可以从私钥解密设备接收问候消息,该问候消息包括例如 (keyid101,8)、(keyid102,64),其指示具有密钥标识符keyid101且 $\bar{n} = 8$ 的第一密钥和具有密钥标识符keyid102且 $\bar{n} = 64$ 的第二密钥。如果在公钥加密设备的密钥高速缓存中这两个密钥都可用或者只有具有IDkeyid102的密钥可用,则可以(例如使用维度 $\bar{m} = 1$)选择使用这个较大的密钥。如果没有密钥可用,则公钥加密设备可以例如从私钥解密设备或其他地方请求keyid101。然后加密可以使用 $\bar{m} = 8$ 。在这两种情况下,传输密钥可以具有相同的长度。

[0217] 图3示意性地示出了公钥加密和私钥解密的示例。在图3中,使用以下符号。

[0218] • parity_bits是指用于纠错的信息

[0219] • obain_parity_bits(k)表示获得k的一些奇偶校验位。例如,可以根据纠错码来生成奇偶校验位。

[0220] • error_correct(k,parity_bits)表示使用parity_bits来纠正k或parity_bits中的潜在错误,从而获得更可能无错误的k的版本

[0221] 根据图3的实施例使用不同类型的帮助者数据。例如,根据实施例,设备20计算传输密钥的奇偶校验位。例如,奇偶校验位与传输密钥一起可以是根据纠错码(例如,BCH码)的码字。例如,如本文所述地利用原始密钥封装码字。如果需要,封装可以包括对帐数据。为了解封装,设备10首先应用对帐数据,从而获得近码字,例如,其中可能存在位错误的码字。可以使用与纠错码相关联的纠错算法来纠正近码字。纠错和对帐数据的使用提高了解密失败的概率,从而允许使用较小的参数并通过较小的密钥大小来提高性能。奇偶校验位和对帐数据的组合是优选组合,从而允许使用较小的公钥矩阵。

[0222] 在协议的实施例中,第一公钥包含 $\bar{n}$ 个向量。密文包括第二公钥u和经封装的数据c。第二公钥矩阵u可以是具有 Z_p 中的元素的维度d的向量。为了使密文的大小最小化,我们可以使用 $\bar{m} = 1$ 。这意味着原始密钥将最多包含 $B\bar{n}$ 个元素。为了优化原始共享密钥的大小,我们将从尽可能多的元素取用B位,由此使用 $\mu = \bar{n}$ 。经封装的数据c对传输密钥进行加密,并且可以具有 $\mu = \bar{n}$ 个元素,使得能够封装长度为 $\kappa = \mu B$ 的传输密钥。B是从每个向量条目中提取的位数。

[0223] 在实施例中,我们想要使密文最小化。可以获得进一步减小密文大小的新见解,即使以较长的公钥为代价也可以,如下所示:

[0224] 第一公钥矩阵包括长度为d的 $\bar{n}$ 个向量。据此能够封装 $\bar{n}B = \kappa + \text{parity_bits_length}$,其中, κ 是传输密钥长度,并且有parity_bits_length个位用作奇偶校验位。

[0225] 由于需要传输其他奇偶校验位,因此向量c将变得更长 $\text{parity_bits_length} \times \log_2 t$ 。然而,由于具有这些奇偶校验位,该方案能够更好地处理解密错误,使得能够选择q和p的较小值。由于p较小,d也可能减小,这是因为我们能够保持相同的安全水平。总之,通过以这种

方式加上纠错码,我们能够进一步减小密文的大小,即使密文以较长的公钥为代价也可以。选择 $B=1$ 是有效的,并且通过使用它,我们需要 $\bar{n} = \kappa + \text{parity_bits_length}$ 。

[0226] 在实施例中,采用以下参数:

[0227]	长期公钥配置	
	d、n	786、1
	q、p、t	2^{16} 、 2^8 、 2^6
	B、 $\bar{n}$ 、 $\bar{m}$	1、 $192+103$ 、1
	μ 、 κ 、#parity_bits	$192+103$ 、192、103

[0228] 103个奇偶校验位允许位纠错。例如,可以使用纠错码Xef,该纠错码Xef允许3位纠错。在Sauvik Bhattacharya等人的“Round5:Compact and Fast Post-Quantum Public-Key Encryption”中描述了Xef。使用Xef的优点是能够在恒定时间内高效地完成解码,由此避免了定时攻击。

[0229] 在该实施例中,密文大小将略大于1KB。这意味着这样的构造能够实现不需要密文分片的非环形配置。重要的是将密文的大小减小到大约1.5kb以下,因为这样可以避免在基于包的通信中产生碎片,在基于包的通信中,例如在互联网上使用的包大约为2kb。

[0230] 请注意,通过缩放引入的噪声量相对较高。在上面的示例中,秘密矩阵元素的16位减少为公共矩阵元素的8位;减少了50%。与之前未给出奇偶校验位的示例相比,将14位减少为12位,减少了大约15%。同样,秘密位的位长与公共位的位长之间的差异已经从2位增加到8位。较高的噪声允许协议的格点部分具有较高的效率,但是以较高的失败率为代价。然后使用奇偶校验位来减少后者。

[0231] 在实施例中, $\bar{m} = 1$ 且 $\bar{n} = \mu = \kappa + \text{parity_bits_length}$ 。例如,其中 $\kappa \geq 128$ 。例如,可以选择奇偶校验位的数量,使得它们能够校正至少3个错误。在实施例中, $\log_2 p / \log_2 q \leq 0.85$,或 ≤ 0.72 ,或 ≤ 0.7 ,或 ≤ 0.6 ,或甚至如以上实施例中那样 ≤ 0.5 ,或甚至更小。请注意,由于原始共享密钥中的所有元素都被使用,例如, $\mu = \bar{n}\bar{m}$,因此没有使用所谓的可靠位。这样的高噪声可以与低 $\bar{m}$ (特别是与 $\bar{m} = 1$ 或 $\bar{m} = 2$)等相结合。

[0232] 图4示意性地示出了公钥加密和私钥解密的示例。图4的实施例包括三个不同的纠错源:安全位、对帐数据和奇偶校验位。

[0233] 在图4中:

[0234] • h表示帮助者数据,其包括对帐位。

[0235] • get_reconciliation(k)是从raw_key k中返回对帐位的函数。

[0236] • reconcile(k,h)是在给定对帐位h的情况下对raw_key k进行对帐的函数。

[0237] • safe_bits()返回两个值:(i)实际可靠值;以及(ii)关键位的位置,由于所获得的值距离量化边界较远,因此关键位的位置能够引起较低的失败概率。由Safe_bits()返

回的实际值以后将用于封装。位置被交换给另一方,使得另一方知道需要哪些位置。

[0238] 有趣的是,当交换码字和从中随机生成的密钥时,可以使用这三种信息源来减少失败的概率。此外,由于能够随机生成码字,因此提高了主动安全性。请注意,可以根据码字导出第二私钥矩阵,以进一步提高主动安全性。该码字可以包括传输密钥和奇偶校验位。这些来源包括可靠位的使用,为原始密钥的系数提取的对帐数据,以及作为码字的部分的纠错冗余信息(例如,奇偶校验位)。

[0239] 例如,在实施例,设备10和20可以在原始密钥上达成一致,例如在 Z_q 中具有 n 个系数的矩阵密钥 k^* 。例如,原始密钥矩阵中的元素可以被映射到传输密钥的部分,例如被映射到一个或多个位。例如, Z_q 中的值的一半可以被映射到0,并且它们的一半可以被映射到1,例如, $B=1$ 。选择可靠位可以通过选择例如距离解码边界最远的一些数量的(例如, μ 个)系数来完成,使得降低出错的概率。

[0240] 密钥对帐数据可以由公钥加密设备例如针对原始密钥(例如,矩阵密钥)的所选择的可靠系数(例如,所选择的 μ 个系数)提取的信息。对帐信息帮助私钥解密设备做出相同的决定,即,是否将原始密钥的特定系数映射到码字的哪个部分。并非只需要对所选择的可靠系数执行该操作,这意味着需要的工作较少。

[0241] 纠错信息可以是奇偶校验位。可以从随机生成的二进制密钥 K 、消息 m 或预密钥中提取奇偶校验位,使得第二设备封装的信息具有一定的冗余性。以这种方式,即使之前发生错误,设备10也能够纠正它们。因此,如果要传输的密钥 K 的长度为 κ 位并且有 $(\mu - \kappa)$ 个奇偶校验位,则这些奇偶校验位帮助设备10确保密钥 K 的 κ 位是正确的。

[0242] 许多量子抗性公钥加密的问题是它们具有一定的失败概率。例如,私钥解密设备和公钥加密设备最初在有噪声的原始密钥上达成一致,然后例如通过对帐数据对有噪声的原始密钥进行对帐。可靠位函数允许公钥加密设备(例如,首先导出原始密钥的一方)识别出私钥解密设备更可能以相同的方式导出原始密钥中的哪些位以及原始密钥中的哪些位不太可能相同。

[0243] 可靠位函数的直接实施方式是为对其采样以获得系数位的系数定义两个或更多个中心点。(例如根据阈值)距离中心点太远的系数可以被丢弃,而其余部分可以被采样到与中心点相关联的值。例如,中心点的数量可以是2的幂。例如,矩阵元素可以取自各种不同的环等。

[0244] 可靠位采样使用以下假设:密钥不需要由环维度给出的所有位。通常,基础矩阵的维数 y 比所需的密钥长度大得多。例如,公钥加密设备可以选择 y 中最可能达成一致的 m 个索引。这些安全系数可以是最接近被映射到零位或一位($k=0$ 和 $k=1$)的系数范围的中心点的那些系数。例如,在对 q 取模的环中,如果系数在范围 $\left[\left\lfloor \frac{q}{4} \right\rfloor - b, \left\lfloor \frac{q}{4} \right\rfloor + b\right]$ 内,则系数可以被映

射到0,如果系数在范围 $\left[\left\lfloor \frac{3q}{4} \right\rfloor - b, \left\lfloor \frac{3q}{4} \right\rfloor + b\right]$ 内,则系数可以被映射到1,反之亦然。如果系数不在这两个范围内,则它不是可靠位。该值 b 部分确定位的可靠性。例如,在这种情况下,可以将其选择为 $q/8$;较小的 b 值提供较高的可靠性,但密钥位较少。在这种情况下,中心点可以是 $q/4$ 和 $3q/4$,或者是其舍入结果。

[0245] 应用上述流程的公钥加密设备获得可靠位和与其对应的密钥位的索引。可以将可

靠索引传达到私钥解密设备,而不能将可靠密钥位传达到私钥解密设备。私钥解密设备能够根据由公钥加密设备指示的索引处的位来获得密钥位。由于这些位更可靠,因此错误率将更低。

[0246] 可靠位函数的其他实施方式能够在文章Hila 5中找到,通过引用将其并入本文。例如,可以应用第3章中的算法。发明人发现,可靠位函数可以应用于多种情况,例如,(例如特别是在矩阵上)具有不同的底层环或对象的情况。

[0247] 在实施例中,两方生成两个原始密钥,例如,近似但不完全等同的矩阵。为了达成精确一致,发送了某个对帐数据。在同一申请人于2016年11月4日向欧洲专利局提交的申请号为16197277.3的专利申请(标题为“REACHING AGREEMENT ON A SECRET VALUE”)中说明了这样做的方案;例如,在实施例中,可以使用第7-10页上的方法进行对帐。也可以采用在引用的专利申请中的其他地方公开的变型。

[0248] 在该申请中,我们将为以下三个函数使用以下符号:

[0249] 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

[0250] $\bar{B} = \log_2 q - B$ 。则有,

[0251] $\lfloor \cdot \rfloor_{B,b_h}: v \rightarrow \lfloor 2^{-\bar{B}} \cdot v \rfloor (\text{mod } 2^B)$

[0252] 直观地, $\lfloor v \rfloor_{B,b_h}$ 提取 $v + 2^{\log q - (B+b_h)}$ 的 B 个最高有效位,其中,第二组成部分是舍入因子,以确保无偏置的舍入错误。 B 指示从符号 v 中提取的位数,并且 b_h 指示帮助者数据位数。在实施例中, q 可以是2的幂。

[0253] 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

[0254] $\bar{B} = \log_2 q - B$ 。则有,

[0255] $\langle \cdot \rangle_{B,b_h}: v \rightarrow \lfloor 2^{-\bar{B}+b_h} \cdot v \rfloor (\text{mod } 2^{b_h})$

[0256] 直观地, $\langle v \rangle_{B,b_h}$ 提取 v 的 $(B+b_h)$ 个最高有效位中的 b_h 个最低有效位。

[0257] 3、对帐函数 $\text{rec}(w, b)$:

[0258] 对于 $q, b_h, B \in \mathbb{Z}, b_h \geq 1, B < \log_2 q - b_h, w \in \mathbb{Z}_q, b \in [0, 2^{b_h})$,

[0259] $\text{rec}(w, b) = \lfloor v \rfloor_{B,b_h}$

[0260] 其中, v 是最接近 w 的元素,使得 $\langle v \rangle_{B,b_h} = b$ 。最接近的元素 w 可以根据Lee距离(例如, $\min(|v-w|, q-|v-w|)$) 来获得。

[0261] 这三个函数能够逐元素地应用于矩阵。在本文中,以上引用的对帐函数用作示例。如上所述,也可以使用以上引用的申请中的对帐方法。能够应用交叉舍入函数来获得对帐数据,并且能够应用舍入函数来获得经过对帐的数据(例如,可靠位)。当以后在对帐函数中使用对帐数据时,经过对帐的数据将被恢复。换句话说: $\text{rec}(w, \langle v \rangle) = \lfloor v \rfloor$, 假设 v 和 w 彼此在阈值距离内。

[0262] 图5示意性地示出了根据实施例的密码系统301的示例。系统301包括私钥解密设备300、公钥加密设备350以及任选的公钥存储库302。例如,第一设备300和第二设备350可

以在被实施在诸如第一设备10、100和/或第二设备20、200之类的设备上。密码系统301可以实施如图4所示的公钥加密系统。密码系统301可以根据需要而(例如通过省去在所述实施例中未使用的元素)适应其他实施例。

[0263] 第一设备300和第二设备350被配置为执行密码协议。它们具有将数据从一台设备安全地传递到另一台设备的能力。各种密码协议可以使用这种相同的能力。作为示例,描述了使用这种能力的两个协议。

[0264] 例如,第一设备和第二设备可以被配置为公钥加密(例如被设计为允许其他设备(例如,第二设备350)对消息(m)进行加密),使得特定设备(例如,第一设备300)能够对经加密的消息进行解密。然而,除了加密设备和解密设备(例如,第二设备350和第一设备300)之外,其他设备都无法获得公钥对消息进行加密的内容。在进行公钥加密的情况下,多个第二设备可以使用第一设备的相同公钥(例如,相同的第一公钥和公共对象)来向第一公共设备发送经加密的消息。即使第二设备使用相同的公钥来对消息进行加密,也无法对另一设备的通信进行解密。

[0265] 第一设备300和第二设备350分别包括通信接口305和355。通信接口被配置为彼此通信。本文描述了例如通过有线或无线网络的通信接口的示例。

[0266] 第一设备300包括被配置为生成第一私钥(r)和根据第一私钥导出的第一公钥(b)的公钥/私钥生成器315。根据私钥导出公钥可以使用公共对象(a),例如,公共矩阵。例如,生成公钥可以涉及与公共对象相乘和/或引入某种类型的噪声,例如按比例缩小相乘结果,加上噪声项等。私钥和公共对象可以是矩阵,例如,在有限域或环上的矩阵。

[0267] 可以短暂地生成第一私钥和第一公钥。例如,后者可以针对密钥协商协议来完成,特别是在第一设备和第二设备使用某种其他认证机制(例如,带外机制,例如,基于证书的认证等)来彼此认证的情况下。也可以生成第一私钥和第一公钥以供长期使用。例如,第一公钥可以被存储在外部公钥存储库302中。公钥存储库302也可以存储公共对象(a)或用于公共对象(a)的种子。

[0268] 第一公钥例如通过通信接口305和355从第一设备300被传送到第二设备350。这可以通过直接通信来完成,也可以例如通过公钥存储库302来间接完成。如果需要,还可以与第一公钥一起传送公共对象(a)。例如,可以通过发送可以根据其生成公共对象(a)的种子来传送公共对象。

[0269] 第二设备350可以包括公钥获得器360,公钥获得器360例如被配置为从公钥存储库302中检索第一公钥。例如,这种类型的获得适合于公钥加密。然而,公钥也可以直接从第一设备获得,例如在电子邮件中可能是越界的。可以存储公钥,直到需要进行公钥加密交换为止。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,可以短暂地生成第一公钥和/或公共对象。

[0270] 第二设备350可以包括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)的公钥/私钥生成器365。与第一私钥(r)和第一公钥(b)相比,第二私钥(s)和第二公钥(u)可以更小,例如具有更少的条目。

[0271] 第二公钥使用与生成第一公钥时相同的公共对象。第一私钥和第二私钥是其各自设备的私钥。如果需要,它们可以与受信方共享,例如用于备份、密钥托管等。公钥和公共对象不一定针对安全性是秘密的;尽管如此,如果需要,它们中的一个或多个仍然可以是针对

第一设备和第二设备私有的。例如,第一公钥只可以与第二设备共享,反之亦然。

[0272] 第二设备350可以包括码字生成器370。码字生成器370被配置为根据纠错码来生成码字。纠错码可以是线性码或非线性码。例如,纠错码可以是BCH码、Reed-Solomon码、Hadamard码等。可以级联多个代码。级联代码是根据两个或更多个较简单代码构成以便以合理的复杂度实现良好性能的纠错码。例如,可以将Hadamard码与BCH码级联。

[0273] 在码字中编码的是用于封装的数据。例如,码字可以被划分为数据部分(例如,数据位)和奇偶校验部分(例如,奇偶校验位)。例如,用于封装的数据可以被包括在数据位中。用于生成码字的一种方法是生成数据部分并根据该数据部分来计算奇偶校验位。例如,可以将具有数据位的数据向量与奇偶矩阵进行矩阵相乘以获得奇偶位,甚至是完整的码字。可以通过组合用于封装的数据与奇偶校验位来获得码字。例如,可以对数据部分和奇偶校验部分进行级联,但是数据位和奇偶校验位的任何排列都可以用于根据对应的纠错码来产生有效的码字。例如,可以交替数据位与奇偶校验位。请注意,对帐数据通常是在单个 q 进制符号上计算的,但奇偶校验数据通常是多个位计算的;请注意, q 远大于2。

[0274] 可以以各种方式使用该码字。还可以通过在第二设备350处(例如通过(例如为此目的而随机生成的)对称密钥))对消息(m)进行加密并将经加密的对称密钥编码在码字中来获得公钥加密。可以使用额外的密钥推导步骤。例如,可以在码字中编码随机预密钥,并且可以根据预密钥来导出加密密钥。例如,推导可以使用密钥推导函数(KDF),例如,散列函数。例如,在后一种情况下,可以将经加密的消息与对该数据进行解密所要求的数据(如下面所讨论的,例如,第二公钥和其他数据)一起从第二设备发送到第一设备。传输密钥可以被直接编码在码字中,或者可以根据码字来导出。

[0275] 有趣的是,码字是独立于第一私钥、第一公钥、第二私钥和第二公钥生成的。因此,该协议提高了抵御主动攻击的抵抗力。攻击者影响共享密钥的概率变小,因为攻击者无法通过选择第一私钥和第二私钥来影响密钥。在实施例中,第二私钥矩阵是根据码字或者根据传输密钥导出的。

[0276] 例如,在消息的情况下,如果消息是根据独立于公钥加密的应用程序(例如,金融或通信应用程序等)生成的,则可以获得独立的生成。例如,可以通过随机生成来获得独立的生成。例如,码字中的密钥或预密钥可以是独立生成的,例如通过使用真正的随机数生成器或者使用伪随机生成器(其使用与第一私钥和第二私钥无关的种子,例如,其本身是随机生成的,或者是预先确定的等)来独立生成。例如,即使在接收到第一公钥之前和/或在生成第二私钥之前,也可以在第二设备处生成码字;这也确保了独立性。

[0277] 第二设备350包括Diffie-Hellman单元375。Diffie-Hellman单元375被配置为根据第一公钥(b)和第二私钥(s)来生成第二原始共享密钥(k^*)。例如,Diffie-Hellman单元375可以被配置为将Diffie-Hellman函数应用于第一公钥和第二私钥。例如,Diffie-Hellman函数可以是相乘的。第二设备350被配置为将其第二公钥传送到第一设备300。第一设备300包括Diffie-Hellman单元325。Diffie-Hellman单元325被配置为根据第二公钥(u)和第一私钥(r)来生成第一原始共享密钥(k'),例如通过应用相同的Diffie-Hellman函数来生成第一原始共享密钥(k')。不幸的是,对于某些类型的Diffie-Hellman函数,第一原始密钥和第二原始密钥可能彼此靠近,但不一定是相同的。发生这种情况的特定概率取决于基础Diffie-Hellman函数。在大多数应用程序中可以接受不同原始密钥的某种概率,然而,

这种概率有多高将取决于应用程序。然而,通常,较低的概率将是优选的。原始密钥可以与私钥和公钥具有相同的数学类型,例如,矩阵。

[0278] 第二设备350包括可靠位生成器380和对帐数据生成器385。可靠位生成器380被配置为将可靠位函数应用于第二原始共享密钥(k^*)以获得可靠索引和根据所指示的系数导出的可靠位。可靠索引指示原始共享密钥的系数。例如,可靠位生成器380可以确定原始密钥中的哪些系数接近采样边界以及原始密钥中的哪些系数不接近采样边界。例如,原始密钥中的在采样边界的阈值内的系数可以被认为不可靠而被丢弃。剩余的可靠系数可以由可靠索引来指示。可以通过对可靠系数进行采样来获得可靠位。

[0279] 在剩余的系数不足的情况下,存在若干概率,例如,终止协议,利用新的第一私钥和/或第二私钥和/或新的公共对象来重新启动协议,导出较短的密钥或者丢弃较少的系数。代替选择阈值内的所有系数,还可以选择预定数量的系数(例如, μ 个系数),并且选择最可靠的系数(例如,前 μ 个最可靠的系数)。

[0280] 实施可靠位的一种方法是采用系数的一个或多个(例如B个)最高有效位)。例如,每个所选择的系数的可靠位数可以是1或2。在一些实施例中,例如,当使用大矩阵时,系数的数量很大,这允许高可靠性,例如B具有低值。对于其他实施例,例如,对于IoT设备,可以使用B的更大值。有限环中的计算可以在对2的幂取模的整数的有限环中进行。后一种选择的优点是,可靠位中的分布更均匀。

[0281] 对帐数据生成器385被配置为针对原始共享密钥的所指示的系数生成对帐数据(h)。对帐数据包括允许减小在第一设备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。例如,应用对帐数据可以使在第一设备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,由此增加了这两者将产生相同的可靠位的概率。码字中的奇偶校验位和对帐数据都用于降低噪声,然而,奇偶校验位是在多个数据位上计算的,而对帐数据是在原始共享密钥中的系数上计算的。对帐数据进一步提高了可靠位的可靠性。

[0282] 一种实施对帐数据的方法是采用系数的紧随被视为可靠位的位的一个或多个位(例如, b_h 个)位。例如,这些位可以是在有效性上紧随这B个位的 b_h 个位。例如,每个所选择的系数的对帐位数可以是1或2。较小的对帐位数具有减少通信开销的优点。不过,也可以有更多的对帐位。

[0283] 第二设备350可以包括封装单元390。封装单元390被配置为通过应用诸如XOR之类的封装函数,利用可靠位来封装码字。该封装可以是一次性焊盘封装。在实施例中,在不知道可靠位的情况下能够从经封装的码字获得的关于码字的信息为零的意义上讲,封装函数获得了完美的安全性。例如,可以在本文描述的其他封装函数之一上使用XOR函数。

[0284] 请注意,封装适用于整个码字,包括数据位和奇偶校验位,而不仅仅是奇偶校验位。此外,封装应用于所生成的数据(例如,消息、密钥、预密钥等),而不应用于根据第一公钥或第二公钥或第一私钥或第二私钥中的一个或多个导出的数据。

[0285] 第二设备被配置为将第二公钥(u)、对帐数据(h)、经封装的数据(c)和可靠索引传送到第一设备。该传送可以例如在密钥协商的情况下响应于接收到第一公钥,或者例如在公钥加密的情况下不响应于接收到第一公钥。

[0286] 第一设备300被配置为从第二设备接收第二公钥(u)、对帐数据(h)和经封装的数

据(c)以及可靠索引。第一设备300包括对帐单元335,对帐单元335被配置为将对帐函数中的对帐数据(h)应用于由可靠索引(safe_bits)指示的第一原始共享密钥(k')中的系数,从而获得可靠位(k)。例如,可以使用对帐位对被指示为可靠的系数进行对帐,然后对其进行采样以获得可靠位。

[0287] 第一设备300包括解封装单元340,解封装单元340被配置为对经封装的数据(c)进行解封装,从而使用可靠位来获得近码字。可以无法直接获得第二设备的码字的原因是,即使具有可靠位和对帐,原始密钥之间的差异仍然无法解析。第一设备300包括纠错器320,纠错器320被配置为将纠错函数应用于近码字以获得码字。

[0288] 最后,可以对码字进行解码,以例如获得数据部分,从而获得消息(m)、密钥(K)或预密钥。在第一种情况下,可以基于该消息来采取某些措施,例如,可以例如在通信器应用程序中显示该消息。在第二种情况下,可以将密钥用于进一步受保护的通信等。在第三种情况下,可以将密钥推导函数应用于预密钥以获得共享密钥。

[0289] 下面给出了一个小而说明性的示例,以说明可靠性和对帐。我们将取 $=2^5=32$ 和 $B=b_h=1$ 。我们将系数写为五位序列,其中,最高有效位在左侧。例如,在实施例中,第二设备可以丢弃系数00000、00001、01110、01111、10000、10001、11110和11111,因为仅对这样的系数进行小的加法或减法将使它们翻转最高有效位。

[0290] 不会被丢弃的系数为00010、00011、……、01101和10010、10011、……、11101。第一列表中的系数将给出为0的可靠位,而最后一个列表中的系数将给出为1的可靠位。这些序列的第二位可以作为对帐数据。所选择的系数的对帐数据会被传送到其他设备,但可靠位不会被传送到其他设备。

[0291] 在第一设备计算其原始密钥之后,它根据由第一设备指示的系数来选择系数。例如,假设第一设备的原始密钥中的系数为01101,并且该系数的对帐数据为0。由于第一设备处的系数的第二位不为0,因此向第一设备指示出错了。与所选择的系数01101最接近的,具有为0的第二位的且不会被丢弃的值是10010。请注意,00111的第二位也为0,但距离所选择的系数01101更远。因此,第一设备将选择1作为这个所选择的系数的可靠位。

[0292] 请注意,如果噪声很大,则该校正可能是错误的;可以想象第二设备的系数为00111。在这种情况下,选择了错误的可靠位。有趣的是,即使有中等量的对帐数据,这些类型的错误也很少见。这意味着,与增加对帐数据的量相比,依靠纠错码来纠正剩余数量的错误更为有效。使Lee距离最小化可以简单地通过以下操作来完成:在增加Lee距离的情况下尝试候选修正系数,直到找到匹配项位置为止。更高级的算法也是可以的,例如,本领域中描述的算法。

[0293] 可靠性与对帐之间存在有趣的协同作用。可能发生的情况是,具有正确对帐数据的最接近的经修改的系数已被公钥加密设备丢弃。具有正确对帐数据的最接近的经修改的系数以及不会被公钥加密设备丢弃的额外约束条件可以具有不同的可靠位。通过考虑这一点,进一步提高了对帐位的效力。例如,继续上面的示例,考虑第二设备获得对帐数据为0的系数01100。最接近的经修改的系数为10000,但未被丢弃的最接近的系数为00111。因此,第一设备恢复可靠位0而不是1。

[0294] 在一些实施例中,公钥加密设备的处理器被配置为:至少基于传输密钥来导出最终密钥,利用该最终密钥对消息进行加密,并且将所述经加密的消息传送到私钥解密设备。

在一些实施例中,私钥解密设备的处理器被配置为:从私钥解密设备接收经加密的消息,至少基于传输密钥来导出最终密钥,并且利用该最终密钥对经加密的消息进行解密。

[0295] 例如,在实施例中,公钥加密设备和/或私钥解密设备可以至少部分地基于将密码散列函数应用于传输密钥来导出最终密钥。作为说明性示例,可以通过将密码散列函数应用于传输密钥以及任选地应用于部分或全部公钥(例如, $G=H(m||pk)$)来根据传输密钥K导出最终密钥,这样的密码散列G可以直接用作最终密钥,或者任选地,可以例如利用经掩蔽的传输密钥c对这样的密码散列的至少部分(例如, $L||rest=G$)进行进一步散列化,以获得最终密钥(例如, $k=H(L||c)$)。

[0296] 进一步设想到以下编号的实施例:

[0297] 1、一种公钥加密设备(20),包括:

[0298] 通信接口,其被配置为与私钥解密设备(10)通信;

[0299] 处理器,其被配置为:

[0300] 获得与所述私钥解密设备相关联的第一公钥矩阵(b),

[0301] 生成传输密钥(K),

[0302] 生成第二私钥矩阵(s),并且根据所述第二私钥矩阵(s)来计算第二公钥矩阵(u),所述第二公钥矩阵(u)具有比所述第一公钥矩阵(b)少的矩阵元素,

[0303] 根据所述第二私钥矩阵(s)和所述第一公钥矩阵(b)来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矩阵(s)与所述第一公钥矩阵(b)之间的矩阵相乘,

[0304] 通过应用封装函数,利用所述第二原始共享密钥的至少部分来封装所述传输密钥(K),从而获得经封装的数据(c),

[0305] 将所述第二公钥矩阵(u)和所述经封装的数据(c)传送到所述私钥解密设备。

[0306] 2、一种私钥解密设备(10),包括:

[0307] 通信接口,其被配置为与公钥加密设备(20)通信;

[0308] 处理器,其被配置为:

[0309] 生成第一私钥矩阵(r),并且根据所述第一私钥矩阵(r)来计算第一公钥矩阵(b),并且允许将所述第一公钥矩阵(b)传送到所述公钥加密设备,

[0310] 从所述公钥加密设备接收第二公钥矩阵(u)和经封装的数据(c),所述第二公钥矩阵(u)具有比所述第一公钥矩阵(b)少的矩阵元素,

[0311] 根据所述第二公钥矩阵(u)和所述第一私钥矩阵(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所述第二公钥矩阵(u)与所述第一私钥矩阵(r)之间的矩阵相乘,

[0312] 使用所述第一原始共享密钥(k')的至少部分对经封装的数据(c)进行解封装以获得传输密钥。

[0313] 3、根据前面编号的实施例中的任一个所述的公钥加密设备或私钥解密设备,其中,

[0314] 所述公钥加密设备的处理器被配置为:

[0315] 获得所述传输密钥(K)的密钥大小,并且根据所述密钥大小来生成所述传输密钥(K),

[0316] 确定所述第二私钥矩阵(s)的矩阵大小以适应对所述密钥大小的所述传输密钥的封装,并且根据所述矩阵大小来生成所述第二私钥矩阵(s),并且

[0317] 将对所述密钥大小和/或所述矩阵大小的指示传送到所述私钥解密设备,并且/或者

[0318] 所述私钥解密设备的处理器被配置为:

[0319] 从所述公钥加密设备接收对密钥大小和/或矩阵大小的指示,并且

[0320] 根据接收到的大小对所述经封装的数据(c)进行解封装以所述获得传输密钥。

[0321] 4、根据前面编号的实施例中的任一个所述的公钥加密设备或私钥解密设备,其中,

[0322] 所述公钥加密设备的处理器被配置为:利用所述传输密钥对消息(m)进行加密,并且将所述经加密的消息传送到所述私钥解密设备,并且/或者

[0323] 所述私钥解密设备的处理器被配置为:从所述私钥解密设备接收经加密的消息,并且利用所述传输密钥对所述经加密的消息进行解密。

[0324] 5、根据前面编号的实施例中的任一个所述的公钥加密设备或私钥解密设备,其中,

[0325] 所述第二原始密钥是矩阵,封装所述传输密钥(K)包括:将所述传输密钥的位加到所述第二原始密钥矩阵的元素的至少部分的最高有效部分,并且丢弃所述第二原始密钥矩阵的元素的至少部分的零或更多个最低有效位,

[0326] 所述第一原始密钥是矩阵,对经封装的数据进行解封装包括:丢弃所述第一原始密钥矩阵的元素的至少部分的零或更多个最低有效位;从所述经封装的数据中减去所述第一原始密钥矩阵的元素的至少部分;并且对减法结果进行舍入。

[0327] 图6a示意性地示出了根据实施例的公钥加密方法(400)的示例。方法400包括:

[0328] 建立(410)与私钥解密设备的通信,

[0329] 获得(420)与私钥解密设备相关联的第一公钥矩阵(b),

[0330] 生成(430)传输密钥(K),

[0331] 生成(440)第二私钥矩阵(s),并且根据第二私钥矩阵(s)来计算第二公钥矩阵(u),第二公钥矩阵(u)具有比第一公钥矩阵(b)少的矩阵元素,

[0332] 根据第二私钥矩阵(s)和第一公钥矩阵(b)来计算(450)第二原始共享密钥(k*),计算第二原始共享密钥包括第二私钥矩阵(s)与第一公钥矩阵(b)之间的矩阵相乘,

[0333] 通过应用封装函数,利用第二原始共享密钥的至少部分来封装(460)传输密钥(K),从而获得经封装的数据(c),

[0334] 将第二公钥矩阵(u)和经封装的数据(c)传送(470)到私钥解密设备。

[0335] 图6b示意性地示出了根据实施例的私钥解密方法500的示例。方法500包括:

[0336] 建立(510)与公钥加密设备的通信,

[0337] 生成(520)第一私钥矩阵(r),并且根据第一私钥矩阵(r)来计算第一公钥矩阵(b),并且允许将第一公钥矩阵(b)传送到公钥加密设备,

[0338] 从公钥加密设备接收(530)第二公钥矩阵(u)和经封装的数据(c),第二公钥矩阵(u)具有比第一公钥矩阵(b)少的矩阵元素,

[0339] 根据第二公钥矩阵(u)和第一私钥矩阵(r)来计算(540)第一原始共享密钥(k'),

计算第一原始共享密钥包括第二公钥矩阵 (u) 与第一私钥矩阵 (r) 之间的矩阵相乘,

[0340] 使用第一原始共享密钥 (k') 的至少部分对经封装的数据 (c) 进行解封装 (550) 以获得传输密钥。

[0341] 如本领域技术人员将显而易见的, 可以有許多不同方式来执行该方法。例如, 能够以所示顺序执行步骤, 但是步骤的顺序也可以改变, 或者一些步骤可以并行执行。此外, 在步骤之间可以插入其他方法步骤。所插入的步骤可以表示例如本文描述的方法的改进, 也可以与该方法无关。此外, 在开始下一步骤之前, 给定步骤可能尚未完全完成。

[0342] 可以使用软件来执行该方法的实施例, 该软件包括用于使处理器系统执行方法 400 和/或 500 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。该软件可以被存储在合适的存储介质 (例如, 硬盘、软盘、存储器、光盘等) 中。该软件可以作为信号沿着电线, 无线地或使用数据网络 (例如, 互联网) 进行发送。可以使该软件可用于服务器上的下载和/或远程使用。可以使用被布置为配置可编程逻辑单元 (例如, 现场可编程门阵列 (FPGA)) 的比特流来执行该方法的实施例, 从而执行该方法。

[0343] 将意识到, 本发明还扩展到适于将本发明付诸实践的计算机程序, 特别是在载体上或载体中的计算机程序。该程序可以是源代码、目标代码、中间源代码和目标代码的形式, 例如部分编译的形式, 或者是适合于在该方法的实施例的实施中使用的任何其他形式。与计算机程序产品有关的实施例包括与所阐述的方法中的至少一个方法的每个处理步骤相对应的计算机可执行指令。这些指令可以被细分成子例程并且/或者被存储在可以被静态或动态链接的一个或多个文件中。与计算机程序产品有关的另一实施例包括与所阐述的系统和/或产品中的至少一个的每个单元相对应的计算机可执行指令。

[0344] 应当注意, 上面提到的实施例说明而不是限制本发明, 并且本领域技术人员将能够设计出许多替代实施例。

[0345] 在权利要求中, 括号内的任何附图标记都不应被解释为对权利要求的限制。动词“包括”及其词形变化的使用并不排除存在权利要求中未提及的其他元件或步骤。元件前面的词语“一”或“一个”并不排除存在多个这样的元件。当在元件列表之前时, 诸如“……中的至少一个”的表述表示从该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”应被理解为仅包括A, 仅包括B, 仅包括C, 包括A和B两者, 包括A和C两者, 包括B和C两者, 或者包括全部A, B和C。本发明可以借助于包括若干不同元件的硬件来实施, 也可以借助于经适当编程的计算机来实施。在列举了若干单元的装置型权利要求中, 这些单元中的若干单元可以由同一件硬件来体现。在互不相同的从属权利要求中记载某些措施的事实并不意味着不能有利地使用这些措施的组合。

[0346] 在权利要求书中, 括号内的引用内容指的是例示实施例的附图中的附图标记或实施例的公式, 由此提高了权利要求的可理解性。这些引用内容不应被解释为对权利要求的限制。

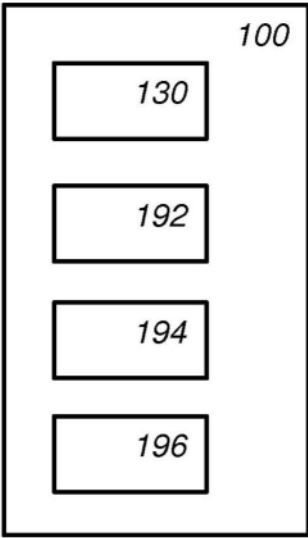


图1a

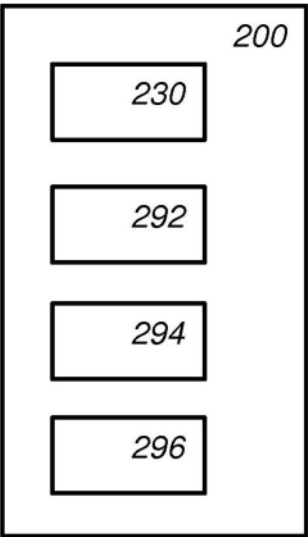


图1b

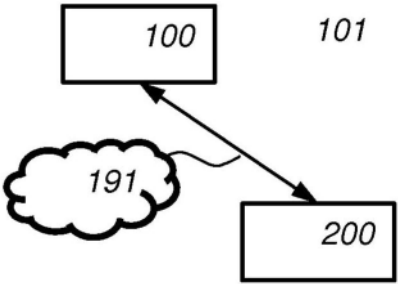


图1c

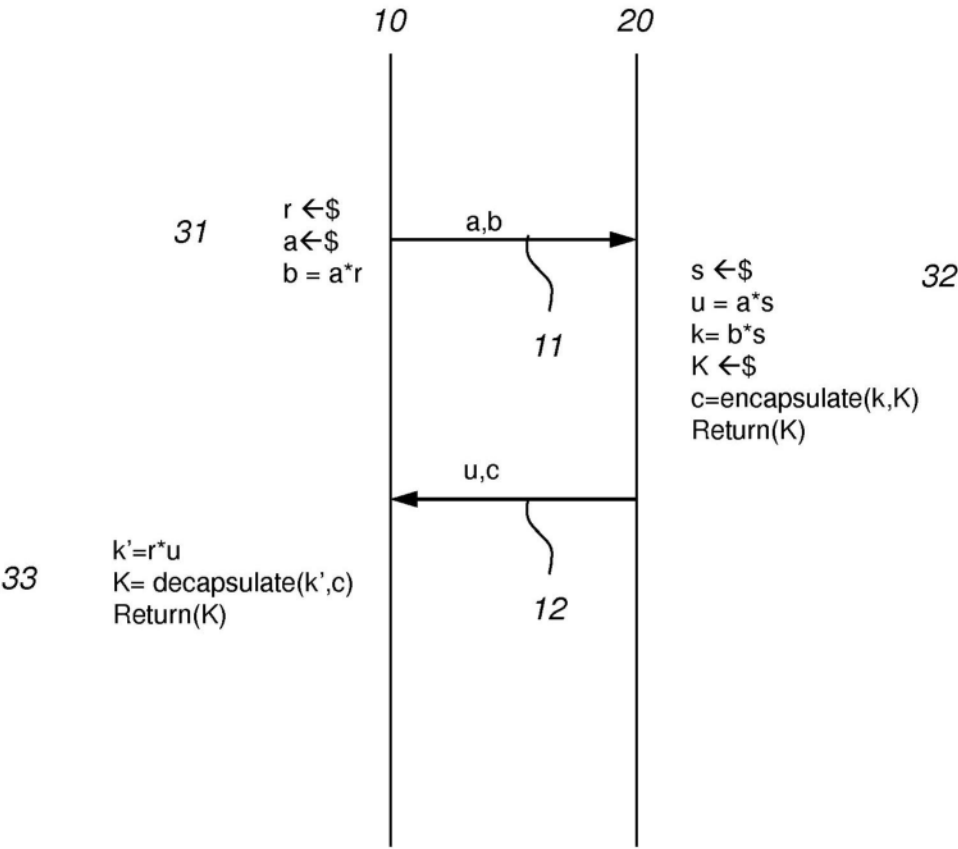


图2a

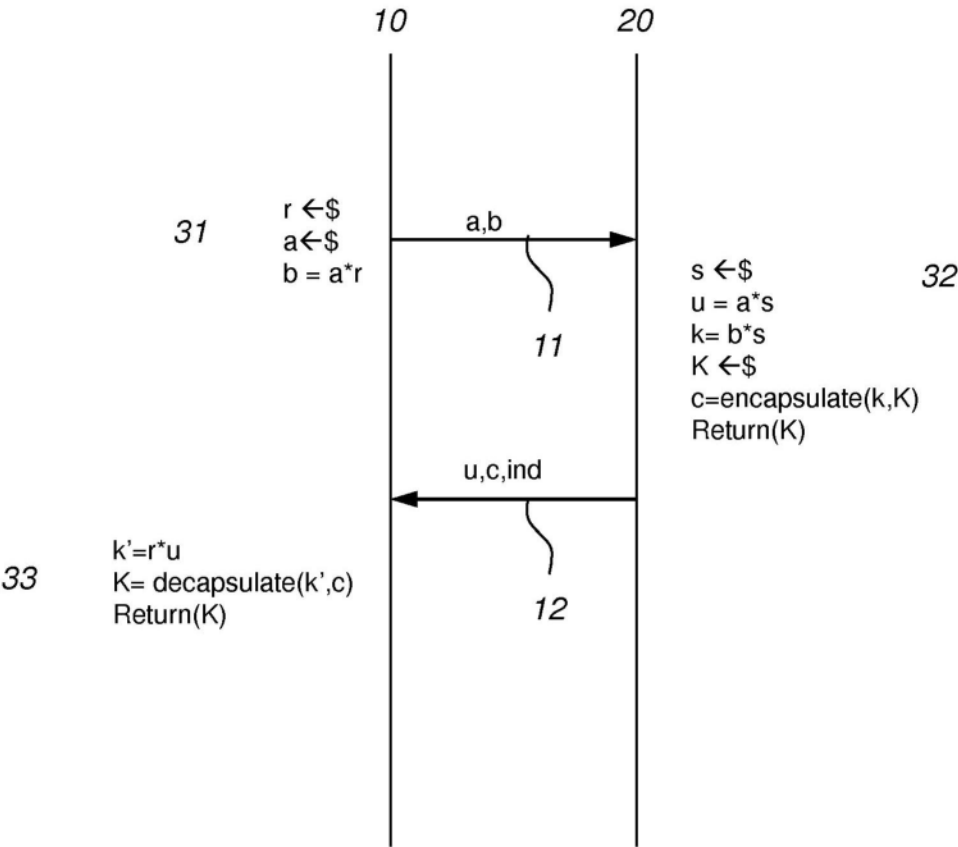


图2b

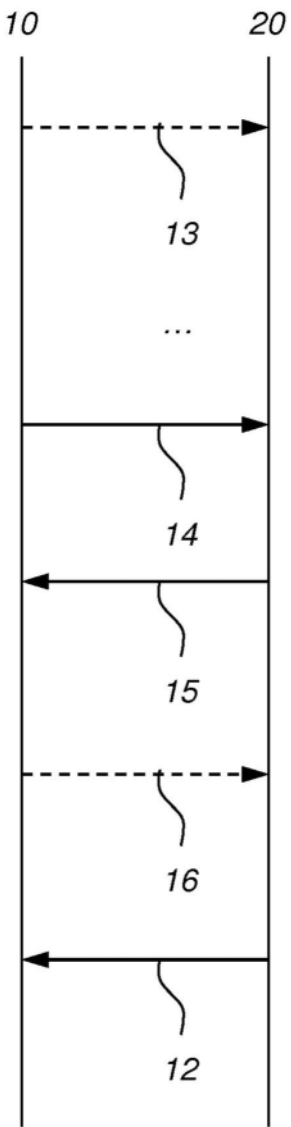


图2c

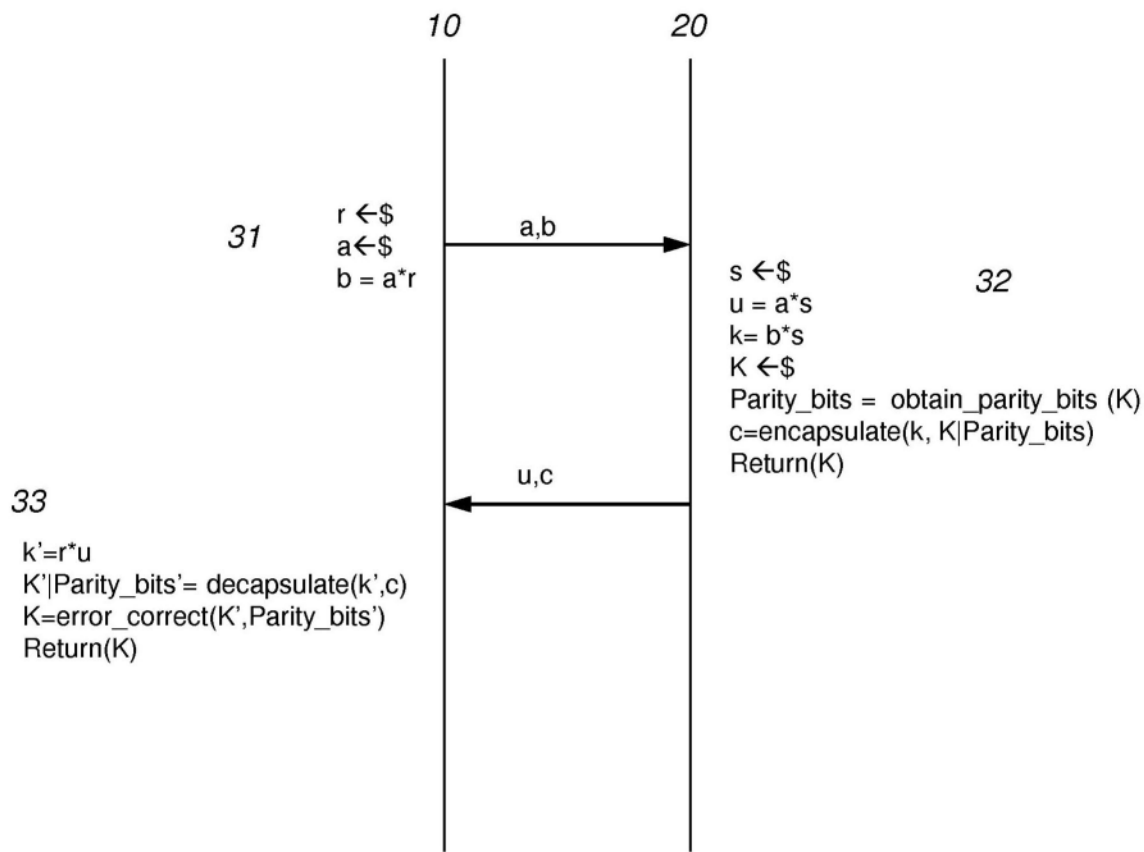


图3

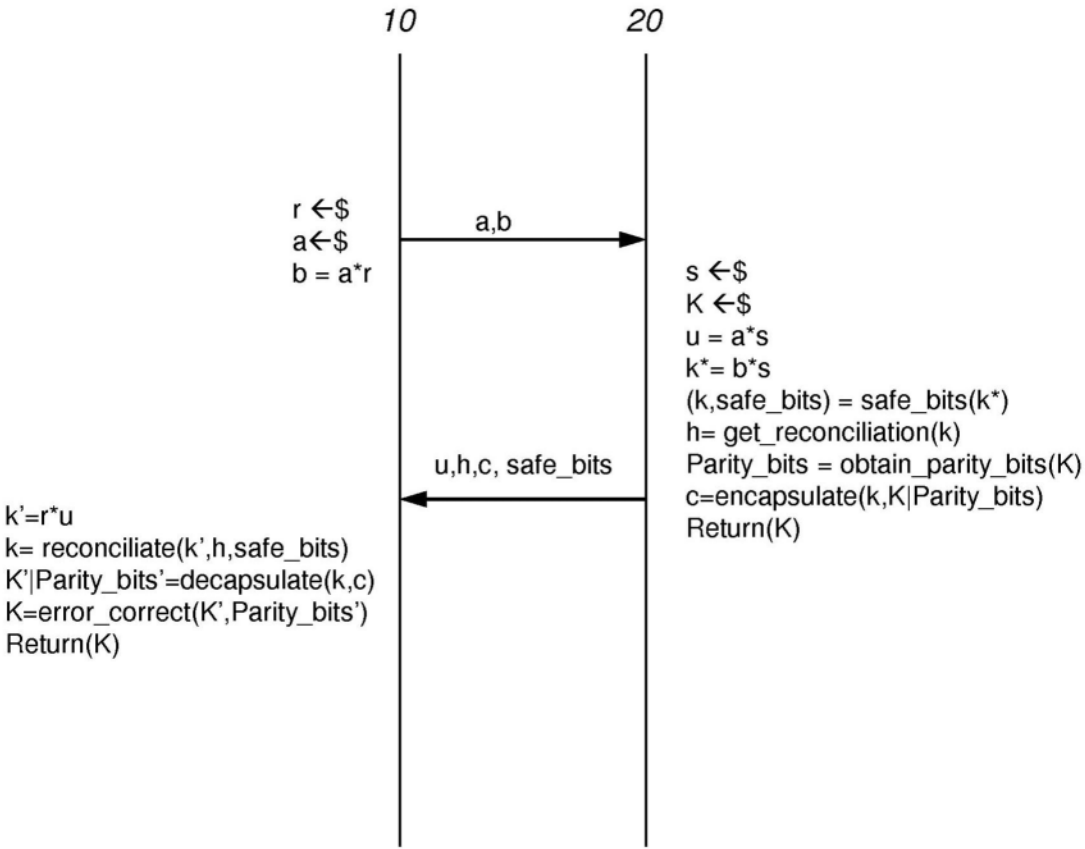


图4

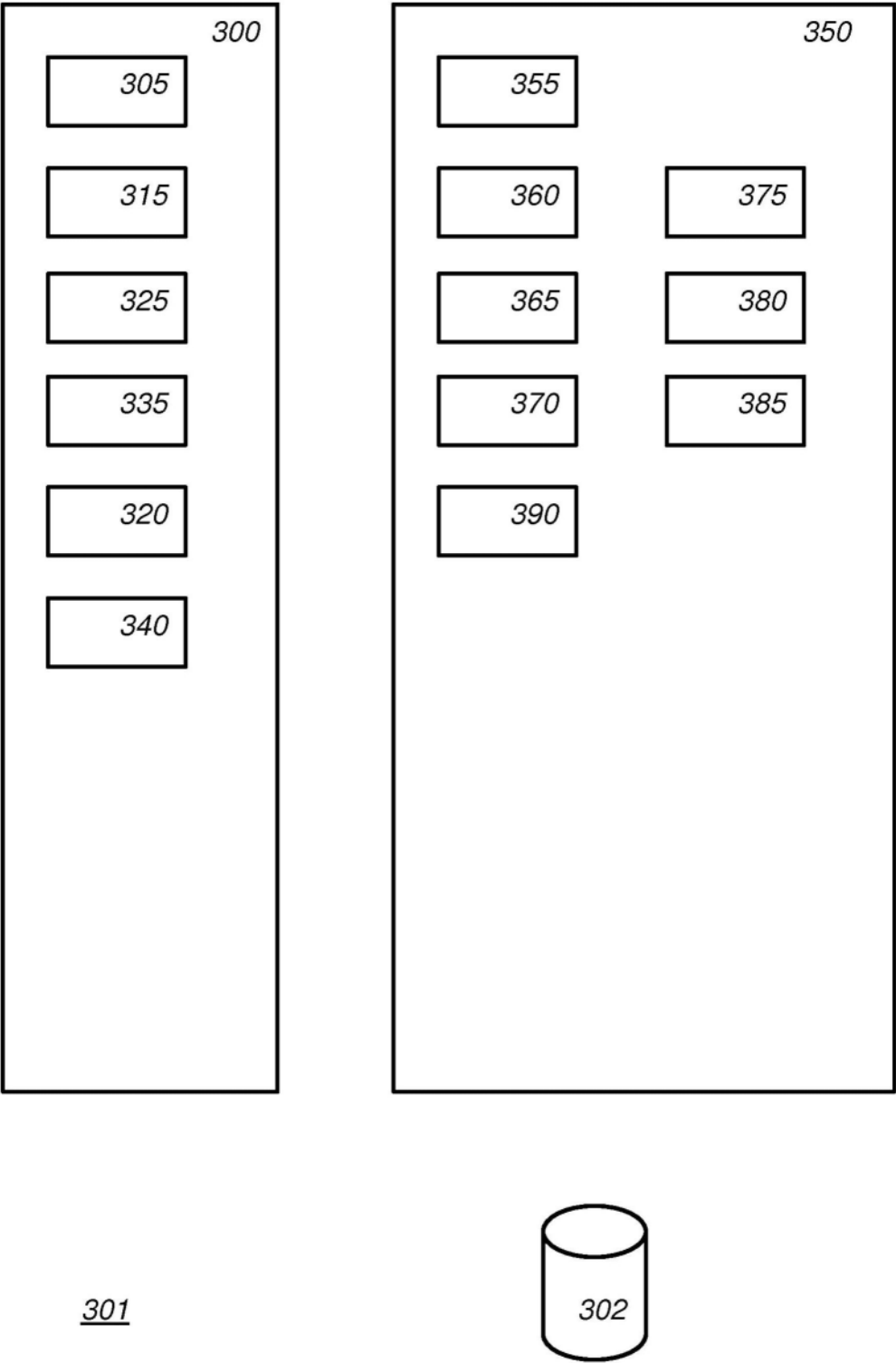


图5

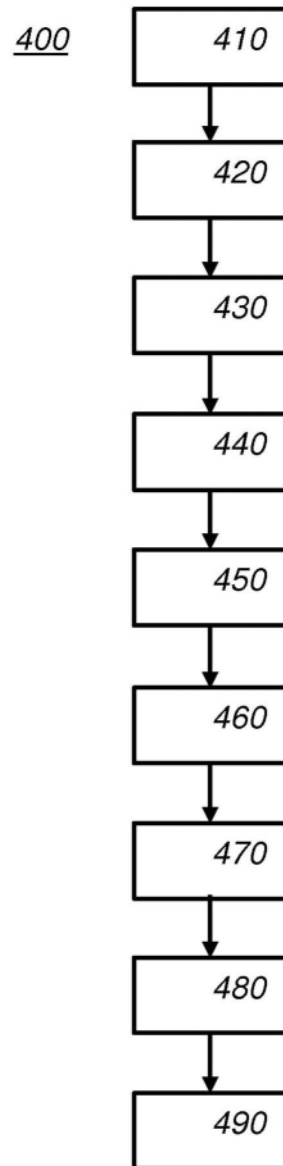


图6a

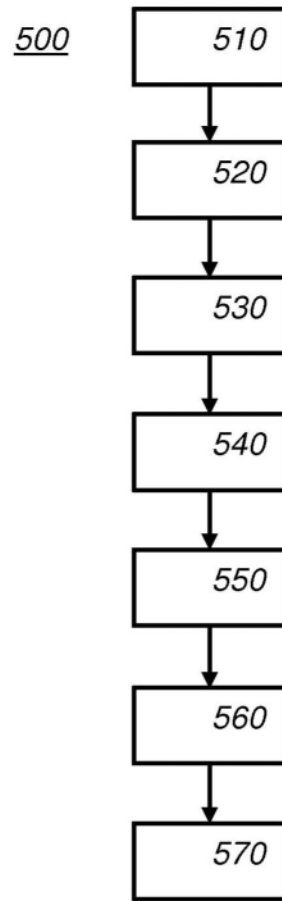


图6b

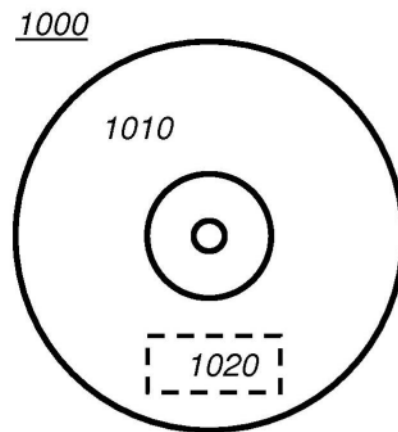


图7a

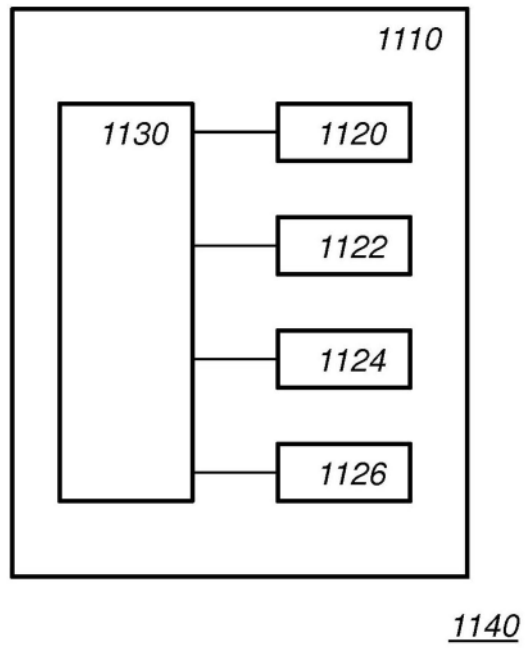


图7b