(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 105027492 B
(45)授权公告日 2019.05.07

(21)申请号 201480011261.1

(22)申请日 2014.02.11

(65)同一申请的已公布的文献号
申请公布号 CN 105027492 A

(43)申请公布日 2015.11.04

(30)优先权数据
61/770503 2013.02.28 US

(85)PCT国际申请进入国家阶段日
2015.08.28

(86)PCT国际申请的申请数据
PCT/IB2014/058891 2014.02.11

(87)PCT国际申请的公布数据
WO2014/132155 EN 2014.09.04

(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.加西亚莫乔恩 S.S.库马 L.M.G.M.托休伊泽恩

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 李舒 景军平

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/30(2006.01)

(56)对比文件
CN 102187615 A,2011.09.14,
WO 2007/149850 A2,2007.12.27,
S. Guo
V. Leung
Z. Qian.A Permutation-Based Multi-Polynomial Scheme for Pairwise Key Establishment in Sensor Networks.《2010 IEEE International Conference on Communications》.2010,

审查员 高焕泽

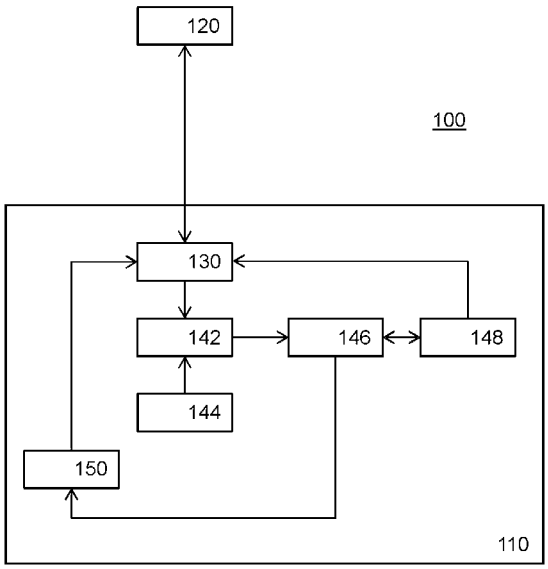
权利要求书3页 说明书16页 附图6页

(54)发明名称

用于确定共享密钥的设备、方法和系统

(57)摘要

提供了一种网络设备(110),所述网络设备被配置成从多项式和第二网络设备(120)的身份号确定与第二网络设备共享的有密钥长度(b)个比特的共享密码密钥。归约算法被用于通过第二网络设备的身份号评估多项式,并对公共模数取模和对密钥模数取模来归约。归约算法包括在多项式的项上的迭代。至少在与多项式的具体项相关联的迭代中,包括第一乘法和第二乘法。第一乘法是在身份号与从多项式的表示获得的具体项的系数的最低有效部分之间,所述系数的最低有效部分由所述具体项的系数的密钥长度个最低有效比特形成。第二乘法是在身份号与从多项式的表示获得的具体项的系数的另外部分之间的第二乘法之间,所述系数的另外部分由所述具体项的系数的不同于所述密钥长度个最低有效比特的比特形成,所述另外部分和所述最低有效部分一起形成比在多项式的具体项的系数中严格地更少的比特。



CN 105027492 B

1.一种第一网络设备(110),被配置成从多项式和第二网络设备的身份号来确定与第二网络设备共享的有密钥长度个比特的共享密码密钥,所述多项式具有多个项,每一项与不同的次数和系数相关联,所述第一网络设备包括:

- 电子存储装置,用于存储针对第一网络设备的本地密钥素材,所述本地密钥素材包括多项式的表示以供第一网络设备在对该多项式的评估中使用,

- 接收机,用于获得第二网络设备的身份号,所述第二网络设备与所述第一网络设备不同,

- 多项式操纵设备(142),被配置成根据归约算法对身份号施加该多项式,以及

- 密钥导出设备(146),用于从归约结果中导出该共享密钥,其中

- 所述归约算法包括在该多项式的项上的迭代,其中与该多项式的具体项相关联的至少一个迭代包括:

- 在身份号与从多项式的表示获得的具体项的系数的最低有效部分之间的第一乘法,所述系数的最低有效部分由所述具体项的系数的密钥长度个最低有效比特形成,

- 在身份号与从多项式的表示获得的具体项的系数的另外部分之间的第二乘法,所述系数的另外部分由所述具体项的系数的不同于所述密钥长度个最低有效比特的比特形成,所述另外部分和所述最低有效部分一起形成比在多项式的具体项的系数中的比特更少的比特,其中所述另外部分是所述具体项的系数的最高有效部分。

2.根据权利要求1所述的第一网络设备,其中,公共模数等于2的指数幂加上偏移,其中所述指数是密钥长度的倍数,并且其中所述偏移的绝对值小于2的密钥长度次幂,多项式的每个系数小于该公共模数。

3.根据权利要求1所述的第一网络设备,其中,密钥模数等于2的密钥长度次幂,身份号小于密钥模数。

4.根据权利要求2所述的第一网络设备,其中,密钥模数等于2的密钥长度次幂,身份号小于密钥模数。

5.根据权利要求2所述的第一网络设备,其中,所述公共模数等于$2^{(a+2)b}-1$,其中α代表该多项式的次数,且b代表密钥长度。

6.根据前述任一项权利要求所述的第一网络设备,其中,在所述多项式的项上的迭代中的每个迭代与多项式项中的特定一项相关联,每个迭代包括:

- 在身份号与从多项式的表示获得的特定项的系数的最低有效部分之间的第一乘法,所述系数的最低有效部分由所述特定项的系数的密钥长度个最低有效比特形成,

- 在身份号与从多项式的表示获得的特定项的系数的另外部分之间的第二乘法,所述系数的另外部分由所述特定项的系数的不同于所述密钥长度个最低有效比特的比特形成。

7.根据权利要求6所述的第一网络设备,其中,所述特定项的系数的另外部分是所述特定项的系数的最高有效部分,所述系数的最高有效部分由所述特定项的系数的多个最高有效比特形成。

8.根据权利要求6所述的第一网络设备,其中,所述另外部分中的比特数是密钥长度的倍数。

9.根据权利要求6所述的第一网络设备,其中,所述另外部分中的比特数随着所述特定

项的次数的减小而减小。

10.根据权利要求9所述的第一网络设备，其中，所述另外部分中的比特数是密钥长度的倍数，并且其中所述倍数等于所述项的次数加上误差控制数。

11.根据权利要求10所述的第一网络设备，其中，所述误差控制数等于1或2。

12.根据权利要求1－5中任一项所述的第一网络设备，其中，所述多项式的系数中的至少一个以预处理形式来表示，在预处理形式下具体项的系数的最低有效部分和所述另外部分被表示在单个比特串中彼此相邻，所述归约算法包括在身份号与所述单个比特串之间的单个乘法以便一起执行第一乘法和第二乘法。

13.一种密钥共享系统，包括用于配置网络设备以进行密钥共享的系统和至少两个根据前述任一项权利要求所述的第一网络设备，所述用于针对密钥来配置网络设备的系统包括：

- 密钥素材获得器，用于以电子形式获得公共模数以及具有整数系数的对称多变量多项式，

- 生成器，用以生成用于所述至少两个第一网络设备中的网络设备的本地密钥素材，所述生成器包括：

-网络设备管理器，用以以电子形式获得用于所述网络设备的身份号以及用于在所述网络设备上电子地存储所生成的本地密钥素材，

-多项式操纵设备，用于通过将身份号代入所述多变量多项式来从双变量多项式确定多项式。

14.根据权利要求13所述的密钥共享系统，其中，用于配置网络设备的系统的生成器被配置成通过以下操作来获得预处理形式的一个或多个系数，即：将所确定的多项式的系数乘以2的密钥长度倍数次幂，接着对公共模数取模归约。

15.一种从多项式和第二网络设备的身份号确定与第二网络设备共享的有密钥长度个比特的共享密码密钥的方法，所述多项式具有多个项，每一项与不同的次数和系数相关联，所述方法包括：

- 存储针对第一网络设备的电子形式的本地密钥素材，所述本地密钥素材包括多项式的表示以供第一网络设备在对多项式的评估中使用，

- 获得第二网络设备的身份号，所述第二网络设备与所述第一网络设备不同，

- 根据归约算法对身份号施加该多项式以获得归约结果，以及

- 从归约结果导出共享密钥，其中，

- 所述归约算法包括在多项式的项上的迭代，其中与多项式的具体项相关联的至少一个迭代包括：

- 在身份号与从多项式的表示获得的具体项的系数的最低有效部分之间的第一乘法，所述系数的最低有效部分由所述具体项的系数的密钥长度个最低有效比特形成，

- 在身份号与从多项式的表示获得的具体项的系数的另外部分之间的第二乘法，所述系数的另外部分由所述具体项的系数的不同于所述密钥长度个最低有效比特的比特形成，所述另外部分和所述最低有效部分一起形成比在多项式的具体项的系数中的比特更少的比特，其中所述另外部分是所述具体项的系数的最高有效部分。

16.一种计算机设备，其包括存储器、处理器和存储在该存储器上的计算机程序，其中

当所述计算机程序在该处理器上运行时使得该处理器实施权利要求15的方法的所有步骤。

17.一种计算机可读介质，包括计算机程序，当所述计算机程序由处理器执行时使得该处理器实施权利要求15的方法的步骤。

用于确定共享密钥的设备、方法和系统

技术领域

[0001] 本发明涉及第一网络设备，其被配置成从多项式和第二网络设备的身份号确定与第二网络设备共享的有密钥长度个比特的共享密码密钥，第一网络设备包括多项式操纵(manipulate)设备，它被配置成对身份号施加多项式。

背景技术

[0002] 倘若通信网络包括多个网络设备，则在成对的这样的网络设备之间设立安全连接是一个问题。在C. Blundo、A. De Santis、A. Herzberg、S. Kutten、U. Vaccaro和M. Yung的“Perfectly-Secure Key distribution for Dynamic Conferences”, Springer Lecture Notes in Mathematics, Vol. 740, pp. 471-486, 1993(被称作“Blundo”)中描述了一种实现此的方式。

[0003] 它假定了中心管理机构，也被称作网络管理机构或可信第三方(TTP)，其生成对称双变量多项式f(x,y)，令系数在具有p个元素的有限域F中，其中p是质数或质数的幂。每个设备具有在F中的身份号，并且由TTP为每个设备提供本地密钥素材。对于具有标识符η的设备，本地密钥素材是多项式f(η,y)的系数。

[0004] 如果设备η希望与设备η’通信，它就使用它的密钥素材生成密钥K(η, η’) = f(η, η’)。由于f是对称的，所以生成相同的密钥。

[0005] 在与本专利申请相同的申请人的题为“KEY SHARING DEVICE AND SYSTEM FOR CONFIGURATION THEREOF”的专利申请中，给出了一种改进的配置网络设备以用于密钥共享的方法。该专利申请具有申请号61/740488和提交日2012年12月21日(通过引用被合并于此)，并且将被称作“配置申请”。

[0006] 在多个网络设备的集合中，每个网络设备具有它自己的唯一身份号和本地密钥素材。本地素材已从秘密多项式导出；后者通常是双变量多项式。在配置申请中，说明了可以如何挑选秘密多项式来获得对某些攻击的较高抵抗。一种这样的攻击具体是共谋攻击，其中多个网络设备尝试重构该秘密多项式。

[0007] 网络设备需要做些工作来建立共享密钥。例如，考虑一对网络设备，每个网络设备接收到为它们而从秘密双变量多项式获得的单变量多项式。当两个网络设备需要在它们之间建立密码密钥时，它们获得另一设备的身份号并将该身份号与它们的本地密钥素材组合以获得共享密钥。

[0008] 一种导出共享密钥的方式是针对其中的每个网络设备将另一网络设备的身份号代入该网络设备的单变量多项式，将代入的结果对公共模数取模归约(reduce)，然后接着对密钥模数取模归约。密钥模数是2的幂，幂的指数至少是密钥长度。

[0009] 因此，在朝向获得共享密钥的第一步中，网络设备可能必须在特定的点实施多项式评估，接着是两次归约。

发明内容

[0010] 将会有利的是具有一种改进的被配置成确定共享密码密钥的网络设备，其要求更少的资源——例如时间和/或存储资源——来获得共享密钥。

[0011] 提供了一种第一网络设备，其被配置成从多项式和第二网络设备的身份号来确定与第二网络设备共享的有密钥长度(*b*)个比特的共享密码密钥。所述多项式具有多个项，每一项与不同的次数和系数相关联。所述第一网络设备包括：电子存储装置、接收机、多项式操纵设备和密钥导出设备。

[0012] 电子存储装置被配置用于存储针对第一网络设备的本地密钥素材，所述本地密钥素材包括多项式的表示以用于稍后的由第一网络设备进行的评估。

[0013] 接收机被配置用于获得第二网络设备的身份号，所述第二网络设备与所述第一网络设备不同。

[0014] 多项式操纵设备被配置成根据归约算法对身份号施加多项式。

[0015] 密钥导出设备被配置用于从归约结果中导出共享密钥。

[0016] 归约算法包括在多项式的项上的迭代。至少一个迭代包括第一乘法和第二乘法。所述至少一个迭代与多项式的具体项相关联。

[0017] 第一乘法是在身份号与从多项式的表示获得的具体项的系数的最低有效部分之间，所述系数的最低有效部分由所述具体项的系数的密钥长度个最低有效比特形成。

[0018] 第二乘法是在身份号与从多项式的表示获得的具体项的系数的另外部分之间，所述系数的另外部分由所述具体项的系数的不同于所述密钥长度个最低有效比特的比特形成，所述另外部分和所述最低有效部分一起形成比在多项式的具体项的系数中严格地更少的比特。

[0019] 第一网络设备和第二网络设备可以是移动设备，比如移动电话、计算机等等。在具体的有利的实施例中，网络设备是照明设备，比如照明器。共享密钥可以被使用来传达与灯的状况有关的信息和/或向灯传输操作命令，比如说将灯开启或关闭。可以用共享密钥对通信加密。

[0020] 除了在要求安全通信的潜在地较大的照明网络中的密钥建立之外，本发明还可以应用于要求设备对之间的安全通信的任何类型的通信网络。

[0021] 网络设备可以是配备有电子通信和计算手段的电子设备。网络设备可以例如以RFID标签的形式被附着到任何非电子对象。例如，这种方法将适合于“物联网(internet of things)”。例如，物体，特别是低成本物体，可以配备有无线电标签，通过无线电标签它们可以通信，例如可以被识别。可以通过诸如计算机这样的电子手段对这样的物体编目录。被盗或损坏的项目将容易地被跟踪和定位。一个特别有前途的应用是包括被配置成确定共享密钥的网络设备的照明器。这样的照明器可以安全地传达其状态；这样的照明器可以被安全地控制，例如开启和/或关闭。网络设备可以是多个网络设备之一，所述多个网络设备各自包括用于发送和接收身份号以及用于发送电子状态消息的电子通信器，并且各自包括被配置用于遵循根据本发明的方法来导出共享密钥的集成电路。

[0022] 在实施例中，本发明的方法可以被用作针对诸如IPSec、(D)TLS、HIP或ZigBee这样的安全性协议的密码方法。具体地，使用这些协议之一的设备与标识符相关联。希望与第一设备通信的第二设备可以生成与给出其标识符的第一设备的共有的成对密钥，并且成对密

钥(或利用例如密钥导出功能由此导出的密钥)可以用在基于预先共享的密钥的以上协议的方法中。具体地,如本发明中限定的设备的标识符可以是网络地址,比如ZigBee短地址、IP地址或主机标识符。标识符还可以是设备的IEEE地址或与设备相关联的私有比特串,以使得设备在制造期间接收与IEEE地址相关联的某种本地建钥(keying)素材。

[0023] 导出共享密钥可被使用于许多应用。典型地,共享密钥将是密码对称密钥。对称密钥可被使用于保密,例如可以用对称密钥来加密外出的或进入的消息。只有可访问身份号和两个本地密钥素材之一这两者(或访问根密钥素材)的设备才能够解密通信。对称密钥可被使用于认证,例如,可以用对称密钥来认证外出的或进入的消息。按照这种方式,可以证实消息的来源。只有可访问身份号和两个本地密钥素材之一这两者(或访问根密钥素材)的设备才能够创建经认证的消息。

[0024] 网络设备可以被配置用于通过网络管理机构(例如可信第三方)的密钥共享。网络管理机构可以从另一个源获得所需的素材,例如根密钥素材,但是也可以自己生成该素材。例如,可以生成公共模数。如果网络管理机构使用配置申请中描述的方法之一,则网络管理机构可以生成私有模数,即使公共模数是系统参数并且被接收到。

[0025] 在实施例中,挑选公共模数N,使得它满足 $2^{(a+2)b-1} \leq N \leq 2^{(a+2)b} - 1$,其中$a$(或$\alpha$)表示多项式的与本地密钥素材相对应的次数,并且$b$表示密钥长度。例如,在实施例中 $N = 2^{(a+2)b} - 1$。用于稍后挑选的模运算可以被特别高效地实现。具有固定的公共模数的优点在于:它不需要被传达给网络设备,而是可以与例如网络设备的系统软件整合。

[0026] 可以依赖于安全性要求和可用的资源来挑选密钥长度(b)个比特。对于普通安全性,128比特就可以足够,对于高安全性,256或者甚至更高是合理的,对于低安全性,80或者甚至64是合理的。网络设备的身份号小于2的密钥长度次幂。

[0027] 对于每个网络设备,由网络管理机构生成与本地密钥素材相对应的多项式。典型地,多项式是单变量的并且是从双变量根多项式导出的。如果根多项式是多变量的,具有比如说k个变量。则网络设备需要接收k-1个不同的身份号来导出在k个设备之间共享的密钥。将接收到的k-1个不同身份号代入网络设备中所表示的多项式的变量。情形k=2对应于两个设备之间的密钥共享。

[0028] 有意思的是,网络设备中用于多项式评估的多项式表示可以是有损的,即,因为表示了过少的信息而不能从该表示中构造多项式。例如,对于多项式的至少一个系数,某组比特——比如说“中间字”,即,不是最高有效字,也不是最低有效字——可以被省去,即,不被存储在该表示中。例如,对于多项式的常数项,仅需要记录最低有效字。字是密钥长度个比特长的。例如,网络管理机构可以在生成本地多项式之后实施以下步骤:针对每个系数选择另外的部分,比如说供在第二乘法中使用的最高有效部分,以及供在第一乘法中使用的最低有效部分。对于至少一个系数,所述另外的部分和最低有效部分具有比对应的项的系数严格地更少的比特。对于每个系数,所述另外的部分和最低有效部分被存储在本地密钥素材中。优选地,系数的中间部分,即,在最高有效部分和最低有效部分之间的部分,不被存储在本地密钥素材中。本地密钥素材被存储在网络设备处。

[0029] 第二网络设备的身份号可以以电子和数字的形式被接收,比如说作为二进制比特串被接收。第二网络设备的身份号与第一网络设备的身份号不同。

[0030] 多项式操纵设备被配置成根据归约算法对身份号施加多项式。所述归约算法被配

置为使得它取得归约结果，所述归约结果对应于以下操作的结果，即：将第二网络设备的身份号代入多项式，并将代入的结果对公共模数取模归约，接着对密钥模数取模归约，密钥模数是2的幂，幂的指数至少是密钥长度。

[0031] 在实施例中，公共模数等于2的指数幂（$2^{(a+2)b}$）加上偏移，其中所述指数是密钥长度的倍数，并且其中所述偏移的绝对值小于2的密钥长度次幂，多项式的每个系数小于公共模数。特别有利的是减去偏移1。在这种情况下，模N运算归约为相加（如以下说明的）。

[0032] 有意思的是，在实施例中，每个迭代具有第一乘法和第二乘法。第一乘法是在接收到的身份号与该项的系数的最低有效b比特字之间，即，第一乘法的尺寸是恒定的。第二乘法是在接收到的身份号与系数的另外部分之间。所述另外部分的尺寸随着项的次数而增大；优选地其单调地增大；更优选地，其严格地增大。例如，尺寸可以是与次数加上误差控制项相等的字数。因此，第二乘法的尺寸可以随次数减小。通过使另外部分的尺寸随次数严格增大，该尺寸仅仅在归约结果的影响大的情况下才大，并且在影响小的情况下小，从而实现了计算资源的大的缩减。

[0033] 发明人发现，具体是系数的最高有效部分和最低有效部分对最后结果，即归约结果，做出贡献。在系数中，这两个部分被中间字分开，所述中间字是不被需要的，因为它们对归约结果没有影响或只是影响很小。在实施例中，使最低有效部分和所述另外部分（即，最高有效部分）聚集在一起。例如，在多项式的系数的至少一个中以预处理形式来表示，在预处理形式下具体项的系数的最低有效部分和所述另外部分被表示在单个比特串中彼此相邻，归约算法包括在身份号与该单个比特串之间的单个乘法，以便一起执行第一乘法和第二乘法。

[0034] 通过乘以2的密钥长度倍数次幂然后对公共模数取模归约，可以以预处理形式高效地获得系数。

[0035] 多个网络设备当中各自具有身份号和针对身份号生成的本地密钥素材的任何一对两个网络设备能够以非常少的资源协商共享密钥。这两个网络设备只需要交换它们的不需要保密的身份号，并实施多项式计算。所需的计算的类型不要求大的计算资源，这意味着该方法适合于低成本的大量类型的应用。

[0036] 如果已从对称多项式获得了本地密钥素材，这允许网络设备对中的两个网络设备都获得相同的共享密钥。如果将模糊数（obfuscating number）加到了本地密钥素材，则本地密钥素材和根密钥素材之间的关系被打乱。

[0037] 在实施例中，对称双变量多项式由网络管理机构生成。例如，对称双变量多项式可以是随机对称双变量多项式。例如，可以使用随机数生成器来把系数选择为随机数。

[0038] 在实施例中，去除共享密钥的多个最低有效比特；例如，去除的比特的数目可以是1、2或更多、4或更多、8或更多、16或更多、32或更多、64或更多。通过去除最低有效比特中的更多个，减小了具有不相等密钥的或然率；具体地，可以将其减小到任何期望的阈值。可以通过遵循数学关系来计算共享密钥相等的或然率，也可以通过经验来确定共享密钥相等的或然率。

[0039] 多项式操纵设备可以以运行在计算机上（比如说集成电路上）的软件实现。多项式操纵设备可以以硬件非常高效地被实现。组合也是可能的。例如，可以通过操纵表示多项式的系数的阵列来实现多项式操纵设备。

[0040] 通过例如使用有线连接或使用无线连接电子地向网络设备发送所生成的本地密钥素材、并使所生成的本地密钥素材存储在网络设备上，可以实现在网络设备处电子地存储所生成的本地密钥素材。这可以在网络设备的集成电路的制造或安装期间(例如测试期间)进行。测试装备可以包括网络管理机构或与网络管理机构连接。这也可以发生在设备成功加入某个操作网络之后(即，在网络访问或自举之后)。具体地，本地密钥素材可以作为操作的网络参数的一部分来分发。

[0041] 可以通过从用于配置网络设备以便密钥共享的系统(例如，网络管理机构设备)电子地接收本地密钥素材，来做到以电子形式获得用于第一网络设备的本地密钥素材。还可以通过从本地存储装置(例如像闪速存储器这样的存储器)取回本地密钥素材，来做到获得本地密钥素材。

[0042] 可以通过从第二网络设备接收身份号(例如从第二网络设备直接接收，例如从第二网络设备无线地接收)来做到获得针对第二网络设备的身份号。

[0043] 公共模数和密钥模数可以存储在网络设备中。公共模数和密钥模数也可以从网络管理机构接收。公共模数和密钥模数也可以隐含在网络设备的软件中。例如，在实施例中，密钥模数是2的幂。可以通过丢弃除了密钥长度个最低有效比特之外的所有比特，来进行对这样的密钥模数取模的归约。首先，将代入的结果对公共模数取模归约，然后进一步对密钥模数取模归约。

[0044] 尽管不是必需的，但是公共模数和密钥模数可以是互质的。这可以通过使公共模数为奇数而使密钥模数为2的幂来实现。在任何情况下，避免密钥模数除尽公共模数，因为那样对公共模数取模归约就可以被省略。

[0045] 在实施例中，第一网络设备接收与设备的标识符相关联的多个(n)本地密钥素材。在该第一设备和第二设备之间生成的密钥被作为通过用第二设备的标识符评估第一设备的多个(n)本地密钥素材中的每一个而获得的多个(n)密钥的组合(例如，拼接)获得。这允许并行地使用该方法。

[0046] 将非对称双变量多项式用作为根建钥素材，即，$f(x,y) != f(y,x)$，允许容纳两组设备的创建，比如，第一组中的设备接收 $KM(Id,y)$，而第二组中的设备接收 $KM(x,iD)$，KM是设备上存储的本地密钥素材。属于同一组的两个设备不能生成共有密钥，但是不同组中的两个设备能。进一步参见Blundo。

[0047] 网络设备的身份号可以作为包含与该设备相关联的信息的比特串的单向函数来计算。单向函数可以是密码散列函数，比如SHA2或SHA3。可以将单向函数的输出截短，使得其适合标识符尺寸。可替换地，单向函数的尺寸小于最大标识符尺寸。

[0048] 本发明的一方面牵涉到一种密钥共享系统，其包括用以配置网络设备以用于密钥共享的系统以及至少两个第一网络设备。用于配置网络设备的系统从多变量根多项式，比如双变量多项式，导出本地多项式，比如单变量多项式。从本地多项式导出多项式的表示。在简单的实施例中，多项式的表示是比如说按照项的次数排序的多项式系数的数字列表。但是在先进的实施例中，在表示中省去了系数的一些部分。

[0049] 在实施例中，用于针对密钥来配置网络设备的系统包括：密钥素材获得器，用于以电子形式获得公共模数以及具有整数系数的对称多变量多项式；生成器，用于生成所述至

少两个第一网络设备的网络设备的本地密钥素材，所述生成器包括：网络设备管理器，用于以电子形式获得用于网络设备的身份号以及用于在网络设备处电子地存储所生成的本地密钥素材；多项式操纵设备，用于通过将身份号代入多变量多项式来从双变量多项式确定多项式。

[0050] 用于配置网络设备的系统还可以进行预处理，例如，在实施例中，用于配置网络设备的系统的生成器被配置成通过将所确定的多项式的系数乘以2的密钥长度倍数次幂并接着对公共模数取模归约，来获得预处理形式的一个或多个系数。

[0051] 这种预处理也可以由网络设备进行，比如说由多项式操纵设备来进行。

[0052] 在用于配置网络设备的系统的实施例中，包括：

[0053] - 密钥素材获得器，用于以电子形式获得私有模数、公共模数以及具有整数系数的对称双变量多项式，公共模数的二进制表示和私有模数的二进制表示在至少密钥长度(*b*)个连续比特中相同，

[0054] - 生成器，用于生成所述至少两个第一网络设备的网络设备的本地密钥素材，所述生成器包括：

[0055] - 网络设备管理器，用于以电子形式获得用于网络设备的身份号(*A*)以及用于在网络设备处电子地存储所生成的本地密钥素材，

[0056] - 多项式操纵设备，用于通过将身份号代入双变量多项式、以代入的结果对私有模数取模归约，来从双变量多项式确定单变量多项式。

[0057] 本发明的一方面牵涉到用于配置网络设备的系统。

[0058] 密钥导出设备可以被实现为计算机(例如集成电路)、运行的软件、以硬件实现、以二者的组合来实现等等，被配置用于从对密钥模数取模归约的结果导出共享密钥。

[0059] 从对密钥模数取模归约的结果导出共享密钥可以包括密钥导出函数的施加，例如在the Open Mobile Alliance(开放移动联盟)的OMA DRM规范(OMA-TS-DRM-DRM-V2_0_2-20080723-A, section 7.1.2 KDF)中定义的函数KDF和类似的函数。导出共享密钥可以包括丢弃一个或多个最低有效比特(在施加密钥导出函数之前)。导出共享密钥可以包括加上、减去或拼接某个整数(在施加密钥导出函数之前)。

[0060] 各自具有身份号和对应的本地密钥素材的多个网络设备可以一起形成通信网络，所述通信网络被配置用于网络设备对之间安全的(例如保密的和/或经认证的)通信。

[0061] 密钥生成是基于ID的，并且允许在设备对之间的成对密钥的生成。第一设备A可以依靠从本地密钥素材和身份号导出密钥的算法。

[0062] 参考作者Song Guo、Victor Leung和Zhuzhong Qian的论文“A Permutation-Based Multi-Polynomial Scheme for Pairwise Key Establishment in Sensor Networks”。

[0063] 本发明的一方面牵涉到一种从多项式和第二网络设备的身份号确定与第二网络设备共享的有密钥长度(*b*)个比特的共享密码密钥的方法。

[0064] 根据本发明的方法可以作为计算机实现的方法被实现在计算机上，或以专用硬件来实现，或以两者的组合来实现。用于根据本发明的方法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用于当在计算

机上执行所述程序产品时实施根据本发明的方法的非暂时性程序代码装置。

[0065] 在优选实施例中，计算机程序包括适于当该计算机程序在计算机上运行时实施根据本发明的方法的所有步骤的计算机程序代码装置。优选地，计算机程序被体现在计算机可读介质上。

[0066] 提供了一种网络设备，所述网络设备被配置成从多项式和第二网络设备的身份号确定与第二网络设备共享的有密钥长度(*b*)个比特的共享密码密钥。归约算法被用于通过第二网络设备的身份号评估多项式，并对公共模数取模和对密钥模数取模来归约。归约算法包括在多项式的项上的迭代。与多项式的具体项相关联的至少一个迭代包括第一乘法和第二乘法。第一乘法是在身份号与从多项式的表示获得的具体项的系数的最低有效部分之间，所述系数的最低有效部分由所述具体项的系数的密钥长度个最低有效比特形成。第二乘法是在身份号与从多项式的表示获得的具体项的系数的另外部分之间，所述系数的另外部分由所述具体项的系数的不同于所述密钥长度个最低有效比特的比特形成，所述另外部分和所述最低有效部分一起形成比在多项式的具体项的系数中严格地更少的比特。

附图说明

[0067] 本发明的这些和其他方面根据下文描述的实施例是明显的，并且将参考下文描述的实施例被阐明。在附图中，

[0068] 图1a和图1b是图示了通信网络的示意框图，

[0069] 图2是图示了生成共享密钥的示意流程图，

[0070] 图3是图示了生成共享密钥的示意序列图，

[0071] 图4a-4f表示各种归约算法，

[0072] 图5是图示了生成共享密钥的另外的示意流程图。

[0073] 应注意，不同的图中具有相同参考数字的项目具有相同的结构特征和相同的功能，或者是相同的信号。在已说明了这样的项目的功能和/或结构的情况下，没有必要在详细描述中对其重复说明。

具体实施方式

[0074] 尽管本发明能有许多不同形式的实施例，然而附图中示出并且将在本文中详细描述一个或多个特定的实施例，要理解本公开内容将被看做是对本发明的原理的示范，而并不打算将本发明限于所示出和描述的特定实施例。

[0075] 图1a是图示了在设立阶段期间的通信网络100的示意框图。图1a示出了网络管理机构160。图1a还示出了多个网络设备，所示出的是第一网络设备110和第二网络设备120。

[0076] 网络设备具有注册阶段和使用阶段。在注册阶段，为参与的网络设备提供身份号和本地密钥素材。本地密钥素材由网络管理机构160提供。

[0077] 网络管理机构160可以例如以电子服务器的形式来实现，并且可以例如在制造期间直接与设备相连。网络管理机构160可以稍后提供本地密钥素材，比方说通过互联网提供。

[0078] 在使用阶段期间，两个(或更多个)网络设备可以通过请求其他网络设备的公开身份号并将所述公开身份号与它们的本地密钥素材组合来建立共享密钥。

[0079] 配置申请提供了关于网络管理机构160可以如何导出本地密钥素材的全面解释。在实施例中，网络管理机构实施一种方法，所述方法包括：以电子形式获得私有模数(p_1)、公共模数(N)和具有整数系数的双变量多项式(f_1)，公共模数的二进制表示和私有模数的二进制表示在至少密钥长度(b)个连续比特上是相同的；生成针对网络设备的本地密钥素材，包括：以电子形式获得用于网络设备的身份号(A)，使用多项式操纵设备通过将身份号代入双变量多项式来从双变量多项式确定单变量多项式，将代入的结果对私有模数取模归约，并且在网络设备处电子地存储所生成的本地密钥素材。

[0080] 换言之，网络管理机构可以从双变量多项式开始，并通过代入网络设备的身份号将所述双变量多项式转换成单变量多项式。通过以某些方式挑选归约和系数等，该过程的安全性可以被改善。最后，对于具体的网络设备，获得存储于其中的具体的单变量多项式。

[0081] 在另外的实施例中，生成针对网络设备的本地密钥素材包括：生成模糊数，并使用多项式操纵设备将模糊数加到单变量多项式的系数以获得被模糊的单变量多项式，所生成的本地密钥素材包括被模糊的单变量多项式。

[0082] 为了从单变量多项式生成共享密钥，网络设备可以进行下面的操作：获得另一网络设备的外部身份号，向其他网络设备发送本地身份号，将外部身份号代入被模糊的单变量多项式对公共模数取模，并对密钥模数取模归约。公共模数和密钥模数是在注册阶段中或在注册阶段之前一起被选择的，并且对于所有参与的网络设备而言是相同的。密钥模数取决于所期望的密钥的尺寸，并且典型地是2的密钥长度次幂。从归约结果对密钥模数取模开始，可以导出共享密钥。导出密钥可牵涉到密钥导出步骤，以在密钥的比特之中分散和/或集中熵，比方说密码散列的应用。

[0083] 不幸地，由于挑选双变量多项式的方式，可能发生共享的密钥不完全相同的情况。这也可以被接受；例如对于ad-hoc网络，一些网络设备不能直接通信可能是没关系的，类似地，对于低成本或低安全性应用，一定的失败率可能是可接受的。通过使用密钥均衡(equalize)过程可以增加具有相等密钥的或然率。将描述经常或总是给出相同结果的若干归约算法。的确，假设有确定共享密钥可能在一小部分情况下失败的事实，则尤为有利的是，现在可以使用不总是给出完全相同的结果、但是以高概率给出完全相同结果的算法。

[0084] 注意，网络管理机构可以使用具有多于2个变量(双变量)的多变量多项式，比如说具有3个、4个或甚至更多个变量的多变量多项式。在这种情况下，多个网络节点需要贡献其身份号以用于导出共享密钥。注意，网络管理机构可以使用非对称多项式，在这种情况下，网络设备被分到多个组中，共享密钥可能只在每组的至少一个成员贡献其身份号的情况下才被导出。

[0085] 例如，网络管理机构可以生成以下形式的针对设备A的建钥素材集合：$KM^{\wedge}(X)=\sum_i KM_i^{\wedge}x^i$，其包括系数$KM_i^{\wedge}$，其中$i=0,\ldots,\alpha$。A能够通过进行以下操作来生成与具有标识符η的另一设备B之间的共有密钥：$K_{AB}=<<KM^{\wedge}(x)|_{x=\eta}>_N>_{2^b}=\ll\sum_i KM_i^{\wedge}\eta'^i>_N>_{2^b}$，其中$N=2^{(\alpha+2)b}-1$。这种对多项式的评估需要在小型嵌入式处理器上被高效地实现。具体参见配置申请的第17-25页，例如关于如何选择参数、根密钥素材和本地密钥素材。

[0086] 高效的多项式评估方法是所谓的霍纳(Horner)法，然而事实证明该方法仍然可以被更进一步优化。多项式评估是通过系数在尺寸大于128比特的大数上来实施的。因此共有

密钥K_{AB}的评估需要在不要求过多存储器来用于中间存储一些大数的情况下进行。此外，多项式是通过模N被评估的，且应当在不实施任何高成本的除法的情况下被实现。本发明提供了优化，以便在具有极小存储器(闪存和RAM)的嵌入式微处理器上实现多项式评估，并且仍然快速实施该多项式评估。

[0087] 对于N的某个具体精细选择接近于$2^{(a+2)b}$。就多项式的次数和密钥长度而言，N的尺寸有助于保护系统免受攻击。由于N接近于2的幂，模运算可以被表示为与小偏移(如果偏移不是1或-1)相加以及可能是相乘。一些优化是和N无关的，比如说将最高次迭代和最低次迭代移出循环，对于每个N的字。

[0088] 图1b是图示了包括多个网络设备的通信网络100的示意框图；所示出的是第一网络设备110和第二网络设备120。我们将例证说明第一网络设备110。第二网络设备120可以相同，或按照相同的原理工作。

[0089] 网络设备110包括收发机130，所述收发机130组合了发送机和接收机以便以有线或无线形式向第二网络设备120发送和从第二网络设备120接收电子(例如，数字)格式的消息。可能地，收发机130还被用来接收本地密钥素材，比如从网络管理机构160或其他可信第三方接收。通过收发机130，接收到另一网络设备的身份号；在本图中是第二网络设备120的身份号。

[0090] 收发机是发送机与接收机的组合，注意，本地导出共享密钥仅需要接收机。如果需要或多或少同时在第一设备和第二设备处导出该共享密钥，则发送机可以便利地被用来发送身份号。

[0091] 网络设备110包括本地密钥素材存储装置144。本地密钥素材存储装置144可以被实现为本地存储器，例如，非易失性存储器，比如闪速存储器，以便存储本地密钥素材。本地密钥素材存储装置144还可以被配置成例如经由收发机130从例如网络管理机构160获得本地密钥素材。本地密钥素材存储装置144被配置成为多项式操纵设备提供所需的参数。由本地密钥素材存储装置144存储的本地密钥素材包括多项式的表示，用于稍后由第一网络设备进行的评估。例如，多项式的表示可以是例如按照次数排序的多项式的系数的列表。然而多项式的表示可以以各种方式被优化；事实证明系数的一些部分对最后结果具有非常小的影响。通过省去那些不太可能对最终结果具有大影响的计算结果(calculation)来优化对共享密钥的确定。不仅可以以这种方式优化计算，还可以通过不存储系数的未被使用的那些部分而优化表示的存储。

[0092] 网络设备110包括多项式操纵设备142，所述多项式操纵设备142被配置成根据归约算法对外部身份号施加多项式以获得归约结果。归约算法被配置为使得它给出归约结果，所述归约结果对应于，即，近似于在以下情况下会获得的结果：将第二网络设备的身份号代入被模糊的单变量多项式，并对结果实施两次归约：首先将代入的结果对公共模数取模归约，其次对密钥模数取模归约。归约结果一致(correspond)，因为它近似其他算法的结果。

[0093] 归约结果常常会等于以下操作的结果，即：将第二网络设备的身份号代入与本地密钥素材相对应的多项式，并对结果实施两次归约：对公共模数取模，然后对密钥模数取模。不幸地，有时二者可能不同。如果它们确实不同，则差异常常被限于一个或几个最低有效比特。优选的是，在少于1%的情况下两个值不同，较不优选地在少于10%的情况下两个值

不同。

[0094] 注意，使用被模糊的多项式或从两个私有模数导出的多项式具有以下特性：在不同的设备上获得的归约结果在罕见的情况下也可能不同(参见配置申请)。因此，在一些罕见的额外情况下另外的差异被引入归约结果中并不被看做是大的额外负担，因为系统将已经被配备成应对这一现实，例如通过密钥均衡或其他解决方案。

[0095] 网络设备110包括用于从对密钥模数取模归约的结果中导出共享密钥的密钥导出设备146。例如，密钥导出设备146可以去除一个或多个最低有效比特。密钥导出设备146还可以施加密钥导出函数。还可能的是，使用第二归约的结果而没有另外的处理。

[0096] 网络设备110包括可选的密钥均衡器 148。注意，可能发生的是，在第一网络设备中导出的共享密钥不等于在第二网络设备中导出的密钥(基于第一网络设备的身份号)。如果这被认为是不期望的，则可以采取密钥均衡协议。

[0097] 网络设备110包括密码元件150，所述密码元件150被配置成将共享密钥使用于密码应用。例如，密码元件150可以在将第一网络设备的消息发送至第二网络设备之前用共享密钥来加密或认证该消息，比如说状态消息。例如，密码元件150可以解密或验证从第二网络设备接收到的消息的真实性。

[0098] 典型地，设备110和120各自包括微处理器(未被示出)，所述微处理器执行存储在设备110和120上的适当软件，例如，软件可以是已被下载并存储在对应的存储器中的，例如，在RAM或诸如闪速存储器这样的非易失性存储器(均未被示出)中的。

[0099] 图2是图示了生成共享密钥200的方法的示意流程图。该方法包括：获得210另一网络设备的外部身份号，向另一网络设备发送220本地身份号，对多项式和接收到的身份号执行230归约算法，导出250共享密钥，向另一网络设备发送260密钥确认消息，确定270密钥是否被确认，以及密码应用280。如果在步骤270中密钥没有被确认，则方法在步骤250中继续，导出新的密钥。例如，步骤250可以每当密钥未被确认时去除一个额外的最低有效比特。

[0100] 对于归约算法存在各种选择，如使用图4a-4f说明的。归约算法的执行可以由多项式操纵设备来进行。可以按照以下说明的算法用软件在微处理器上进行该操作。

[0101] 步骤250、260和270一起形成了密钥均衡协议。例如，在步骤260，可以将随机数(nonce)和在步骤250中导出的共享密钥下随机数的加密发送至第二设备。在步骤260，从第二设备接收消息。接收到的消息可以简单地说：接收到的密钥确认消息表明密钥不相等。接收到的消息也可以包含密钥确认消息。在后一种情况下，第一网络设备验证密钥确认消息，并在密钥相等的情况下建立。如果不相等，则例如通过删除最低有效比特来导出新的密钥。

[0102] 如对于本领域技术人员来说将明显的是，许多执行该方法的不同方式是可能的。例如，步骤的次序能够改变，或者一些步骤可以并行执行。而且，在步骤之间可以插入其他方法步骤。插入的步骤可以代表比如本文描述的方法的细化，或者可以与该方法无关。例如，可以至少部分并行地执行步骤210和220。而且，给定的步骤可以在下一步骤开始之前尚未完全完成。

[0103] 图3以示意的形式示出了在两个网络设备(设备A和B)生成共享密钥时在它们之间的可能的消息序列。时间向下进行。在步骤310，网络设备A将它的身份号发送至设备B。在步骤320，设备B发送它的身份号和针对共享密钥(K1)的密钥确认消息，所述共享密钥(K1)是设备B基于身份号A及设备B的本地密钥素材而导出的。在步骤330，设备A发现它们没有生成

相同的密钥。设备A删除了一个最低有效比特(比如整数除以2)以获得密钥K2。在步骤330，设备A发送新的密钥确认消息。以这种方式，A和B交换密钥确认消息340直到它们在步骤350达到相同的密钥。在步骤350，设备A向设备B发送密钥确认消息。设备B能够验证它们已达到相同的密钥。在步骤360，设备B发送对此的确认，这可以是经认证的消息或密钥确认消息等等。在步骤370，设备A发送使用现今相等的共享密钥加密(比如说使用AES)和/或认证(比如说使用HMAC)的消息M1。

[0104] 以下算法给出了这个办法的可能的实现，即，由设备A和设备B运行的用于相互的密钥商定和会话密钥导出的协议。

[0105]

```
Set l=L
Set continue=TRUE
Set Length = b-l
Generate a b-bit key K
While(continue AND (Length>MINIMUM_LENGTH)){
        K = K>>l
        Perform Mutual authentication handshake with B based on K
        If handshake successful, then{
                continue=FALSE
        }}else{
                Length = b-l
                }
```

[0106] 该协议去除了用比如本文中描述的密钥共享算法生成的比特串的多个比特并且实施认证握手，例如，挑战-响应。认证握手可以包括密钥确认消息。如果认证握手没有成功，则去除几个额外的比特，并以此类推直到握手被成功实施或者密钥变得太短。协议能够以多种方式被修改，例如，通过取决于迭代而去除可变数目的比特或总是要求固定数目的步级，使得观察协议的执行的偷听者不会获取与A和B之间共享的共有密钥的长度有关的任何信息。这个办法具有的优点是，它确保了共享密钥尽可能的长，然而它具有的潜在缺点是，它要求多次交换以便商定共有密钥。另一方面，对于大多数应用这不会是个大问题，因为对于大多数设备对而言，密钥将会是相等的或仅有几个比特不同，且只有一设备对会得到有相对大量的不同最低有效比特的密钥。这是从所生成的密钥的特性得出的。

[0107] 存在其他方式来为两个设备得到相同的密钥，例如，如在配置申请中描述的。

[0108] 贯穿图4a-4f地使用以下约定：执行归约结果的网络设备是第一网络设备，贡献其身份号的网络设备是第二网络设备，b代表密钥长度，a代表多项式的次数(有时在文本中写成a)，$KM_{\eta,j}$代表与对应于第一网络设备的多项式的次数j的项相对应的系数，η是第一网络设备的身份号，η'是第二网络设备的身份号，N是公共模数。符号$\langle \dots \rangle_c$代表括号中的数字对c取模的模归约。符号$\gg c$代表右移c比特，即，除以2^c，下舍入到下一个整数。

[0109] 词语input、output、for、end for、return是在计算机算法领域中标准的。

[0110] 在该示例中使用有利的公共模数$N = 2^{(a+2)b} - 1$。该特别的模数允许特别的快速

且简洁的归约。可以针对不同的模数采用这些算法，尤其是在公共模数等于2的指数幂（$2^{(a+2)b}$）减去（正）偏移时，其中所述指数是密钥长度的倍数，并且其中所述偏移的绝对值小于2的密钥长度次幂。当偏移不是1而是更大时，比如说3，最高有效部分被加到最低有效部分偏移次数（offset times）而不是一次。如果偏移是被加上而不是减去，则最高有效部分被加到最低有效部分。

[0111] 作为示例，人们可以取a=2并且b=128。对于更高的安全性，可以使用更大的值，比如说a=4或6。

[0112] 图4a以所谓的伪码形式图示了可以如何获得归约结果。

[0113] 第3行和第5行示出了在由系数$KM_{\eta,j}$给出的多项式的项上的迭代。在每个迭代中，中间值“key”与新系数相乘。这种对密钥$\ll \sum_i KM_i^A \eta'^i >_N >_{2^b}$的评估的实现使用所谓的霍纳法。

[0114] 图4b的算法类似于图4a的算法，但是利用了所使用的模数的特别形式。通过使用N是$N = 2^{(\alpha+2)b} - 1$的特殊形式这一事实来优化步骤$temp \leftarrow \langle key \times \eta + KM_j \rangle_N$。因此，如果我们表示$R$=$key \times \eta$，则R可以被分成两部分 $R = R_1.2^{(\alpha+2)b} + \mathrm{R}_0$，其中$\mathrm{R}_0$是R的$2^{(\alpha+2)b}$个最低有效比特（lsb），而$\mathrm{R}_1$是R的其余MSB。鉴于此，我们可以计算$\langle R \rangle_N = \langle R_1.2^{(\alpha+2)b} + \mathrm{R}_0 \rangle_N = R_1 + \mathrm{R}_0$，因为$\langle 2^{(\alpha+2)b} \rangle_N = 1$。确切地说：是$\langle R_0 + R_1 \rangle_N$等于$R_0 + R_1$，如果它不是过大，即小于N的话。更确切地说，人们可以再一次对N取模归约，并且这么做给出了近似。然而R_1相比于N来说非常小，所以因没有进行二次归约而引入误差的或然率较小。取而代之地，人们还可以在步骤7之后进行模N归约（以相同的技法），并且只有那时才应用步骤8。

[0115] 如果$N = 2^{(\alpha+2)b} -$偏移，则会获得类似的优化。其中偏移相比于N来说小，比如说大于0但是小于密钥模数（2^b）。

[0116] 图4c避免了不必要的计算。通过不实施对最终结果没有影响或影响很小的中间计算，可以改进图4a和图4b的归约算法的性能。在图4c中，利用了以下事实：第一迭代和最后迭代要求更少的计算。在这种设计中，还使用以下表达式$R_j = key \times \eta' + KM_j$消除了mod N归约，因此$\langle R_j \rangle_N = \langle R_{j,1} \times 2^{(\alpha+2)b} + R_{j,0} \rangle_N \approx R_{j,1} + R_{j,0}$，其实现要求比先前那个更少的计算。

[0117] 这种优化使用了$\eta \leq 2^b - 1$并且$KM_j \leq 2^{(\alpha+2)b} - 1$的事实。因为$(key \times \eta' + KM) \leq 2^{(\alpha+3)b} - 2^b < 2^{(\alpha+3)b} - 1$，所以运算$key \leftarrow \langle key \times \eta' + KM_j \rangle_N$可以被高效地实施。

[0118] 因此，key可以被表示为$key = R_1.2^{(\alpha+2)b} + \mathrm{R}_0$，其中$R_1 \leq 2^b - 1$。然后通过N归约是如之前一样的简单相加，但是总是用b比特。图4a、图4b和图4c的算法不具有以下特征：身份号被用在与系数的另外部分和最低有效部分的第一和第二乘法中，所述另外部分和最低有效部分一起形成了比完整系数小的部分，即，多项式的某个部分未被使用。归约算法4a-4c被包括以便与算法4d-4f比较。

[0119] 图4d降低了数据存储要求。在生成密钥时并不要求多项式系数的全部比特。该算法需要仅存储将被使用的那些比特。这个办法还导致所要求的计算的数目的减少。符号 MSB_c 代表c个最高有效字。符号 LSB_c 代表c个最低有效字。字是密钥长度(b)个比特宽的。

[0120] 图4d在第3行和第10行示出了在多项式 KM_η 的项上的迭代。在该具体实施例中，每个迭代与多项式的具体项相关联；迭代依次与次数a-1至1相关联。与次数a和0相对应的迭代是在循环外部实施的。

[0121] 第5行示出了在身份号(η')与从多项式的表示获得的具体项的系数的最低有效部分之间的第一乘法。系数的最低有效部分由所述具体项的系数的密钥长度个最低有效比特形成。

[0122] 第4行示出了在身份号与从多项式的表示获得的具体项的系数的另外部分之间的第二乘法，所述系数的另外部分由所述具体项的系数的不同于所述密钥长度个最低有效比特的比特形成。

[0123] 注意，对于大多数迭代而言，所述另外部分和所述最低有效部分一起形成比在多项式的具体项的系数中严格地更少的比特；事实上它们具有比多项式的具体项的系数更少的字。未被使用的系数也不需要被存储。

[0124] 注意，在每个迭代中，最低有效部分正好是有密钥长度个比特的一个字。然而所述另外部分中的比特数在循环中减少，即，随着次数而减少。

[0125] 所述另外部分中的字数是次数(j)加上误差控制数(red)。这里误差控制数被挑选为1。误差控制数确定了归约算法的结果与图4a的算法的结果完全相同的可能性。为了降低在第一网络设备和第二网络设备之间得到不相等结果的概率，可以增大误差控制数，比如说增大到2。更大的值是可能的，然而概率随着误差控制数而指数地降低。

[0126] 该算法进一步利用了以下事实：并不是相乘的 $KM_j \times \eta'$ 的所有部分都对密钥的最终结果做出贡献。一些部分具有非常微小的效果(由于进位(carry))，但是这些误差在共享密钥的生成期间能够被校正，如在图2和图3中说明的。

[0127] 图4e如图4d的算法一样也尝试降低数据存储要求。尽管这种设计必须存储图4d的算法并不要求的一些额外比特，但它是有利的，因为要求更少的中间计算，所以实现将会更快。

[0128] 在第4行，获得另外的部分，并且在第5行示出了第二乘法。在第6行实施与在前次迭代中已在key中引入的最低有效部分的第一乘法。在第5行，实施第二乘法。

[0129] 图4d的优化需要在每个迭代中从 KM_j 跟踪正在使用的比特的量，并且要求额外的指针管理。图4e的算法减小了对管理存储器的需要。这种优化在存储器方面以及在时钟周期的数量方面更高效。

[0130] 图4f图示了另外的归约算法，其要求对系数的预计算步骤。该另外的归约算法既具有低数据存储要求，又比图4e的算法更快速。一份建钥素材如下地生成：

[0131] $K'_\eta(x) = \sum_{i=0}^{\alpha} \langle KM_i 2^{\alpha b} \rangle_N x^i = \sum_{i=0}^{\alpha} KM'_i x^i$ ，

[0132] 因此每个KM_i'具有特殊形式，这使得这个办法更快速，因为选择MSB和LSB的指令可被跳过。于是，希望生成与第二网络设备η'的密钥的网络设备η可以将密钥计算为：

[0133] $$K_{\eta,\eta'} = \langle \frac{KM_i'(\eta')}{2^{ab}} \rangle_{2^b}$$ 。

[0134] 这种变换具有的效果是，在KM_i'中，具体项KM_i的系数的最低有效部分和所述另外部分被表示在单个比特串中彼此相邻。通常，最低有效部分和最高有效部分被多个中间字彼此分隔开，随着次数越低，该中间部分越大。由于该变换，可以在单个步骤中实施第一乘法和第二乘法。

[0135] 在图4f中使用的系数已按照这种方式被变换。因此，第3行中的乘法一起实施了第一乘法和第二乘法。注意，优选地由TTP进行该变换，并且网络设备将这些变换后的系数存储在本地密钥素材存储装置中。

[0136] 下表给出了对后面的归约算法的相对优势的指示。在闪存和针对动态存储器而用的RAM中实现这些算法。以CPU周期来测量执行时间。用于运行测试的配置是：α=6，b=32，以及32-比特CPU(ARM Cortex-M3)。图4a和图4b的算法比以下给出的示例相对更差。

[0137]

归约算法	闪存尺寸	Ram尺寸	执行时间
图4c	828	36	2521
图4d	892	36	2043
图4e	828	36	1742
图4f	716	36	1283

[0138] 图5再次以流程图的形式图示了用于从多项式和第二网络设备的身份号确定与第二网络设备共享的有密钥长度(*b*)个比特的共享密码密钥的方法，所述多项式具有多个项，每个项与不同的次数和系数相关联。

[0139] 在步骤510，针对第一网络设备以电子形式存储本地密钥素材，所述本地密钥素材包括多项式的表示以用于由第一网络设备进行的稍后的评估。在步骤520，获得第二网络设备的身份号，第二网络设备与第一网络设备不同。在步骤530，根据归约算法对身份号施加多项式以获得归约结果。在步骤540，从归约结果导出共享密钥，比如通过诸如KDF这样的密钥导出算法导出。此外，可以实施密钥均衡算法。步骤530包括归约算法，这由至步骤522、524和526的虚线箭头图示。

[0140] 在步骤522，开始在多项式的项上的迭代，至少一个迭代与多项式的某个具体项相关联。在步骤524，在身份号与从多项式的表示获得的具体项的系数的最低有效部分之间实施第一乘法，所述系数的最低有效部分由所述具体项的系数的密钥长度个最低有效比特形成。

[0141] 在步骤526，在身份号与从多项式的表示获得的具体项的系数的另外部分之间实施第二乘法，所述系数的另外部分由所述具体项的系数的不同于所述密钥长度个最低有效比特的比特形成，所述另外部分和所述最低有效部分一起形成比在多项式的具体项的系数中严格地更少的比特。

[0142] 如对于本领域技术人员来说将明显的是，许多执行该方法的不同方式是可能的。

例如，步骤的次序能够改变，或者一些步骤可以并行执行。而且，在步骤之间可以插入其他方法步骤。插入的步骤可以代表比如本文描述的方法的细化，或者可以与该方法无关。例如，通过创建其中所述另外部分和最低有效部分相邻的数，可以一起执行步骤524和526。而且，给定的步骤可以在下一步骤开始之前尚未完全完成。

[0143] 可以使用软件来执行根据本发明的方法，所述软件包括用于使处理器系统实施方法500的指令。软件可以仅包括由系统的具体子实体采取的那些步骤。软件可以被存储在合适的存储介质中，比如硬盘、软盘、存储器等等。软件可以作为信号沿着线、或无线地、或使用例如互联网这样的数据网络而被发送。可以使软件可用于下载和/或可用于在服务器上远程使用。

[0144] 将认识到，本发明还延伸到计算机程序，尤其是在适于把本发明投入实践的载体上或载体中的计算机程序。程序可以具有以下形式：源代码、目标代码、码中间源和目标代码，比如部分编译的形式，或者具有适合于用在根据本发明的方法的实现中的任何其他形式。与计算机程序产品有关的实施例包括计算机可执行指令，所述计算机可执行指令对应于所阐述的方法中至少一个方法的处理步骤的每一个。这些指令可以被细分为子例程和/或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计算机可执行指令，所述计算机可执行指令对应于所阐述的系统和/或产品中至少一个系统和/或产品的装置的每一个。

[0145] 应注意，上述实施例是例证说明而非限制本发明，并且本领域技术人员将能够设计出许多可替换的实施例。

[0146] 在权利要求中，置于圆括号之间的任何参考数字不应被解读为限制权利要求。动词“包括”及其变形的使用并不排除权利要求中记载的那些元件或步骤以外的元件或步骤的存在。元素前面的冠词“一”或“一个”（“a”或“an”）并不排除多个这样的元素的存在。可以利用包括若干相异元件的硬件以及利用合适地编程的计算机来实现本发明。在列举了若干装置的设备权利要求中，这些装置中的若干个可以由硬件的同一项来体现。仅仅是在互不相同的从属权利要求中陈述了某些措施的事实并不表明这些措施的组合不能被使用来获益。

[0147] 图1a、图1b和图2的参考数字的列表：

[0148] 100 通信网络

[0149] 110 第一网络设备

[0150] 120 第二网络设备

[0151] 130 收发机

[0152] 142 多项式操纵设备

[0153] 144 本地密钥素材存储装置

[0154] 146 密钥导出设备

[0155] 148 密钥均衡器

[0156] 150 密码元件

[0157] 160 网络管理机构

[0158] 210 获得另一网络设备的外部身份号

[0159] 220 向另一网络设备发送本地身份号

[0160] 230 执行归约算法

[0161] 250 导出共享密钥

[0162] 260 向另一网络设备发送密钥确认消息

[0163] 270 密钥被确认？

[0164] 275 否

[0165] 280 密码应用

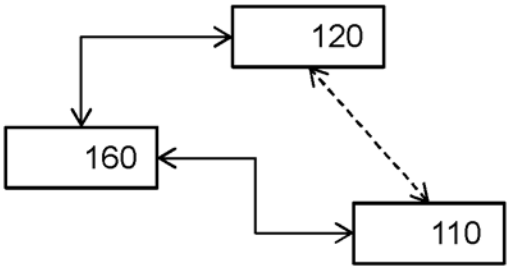


图 1a

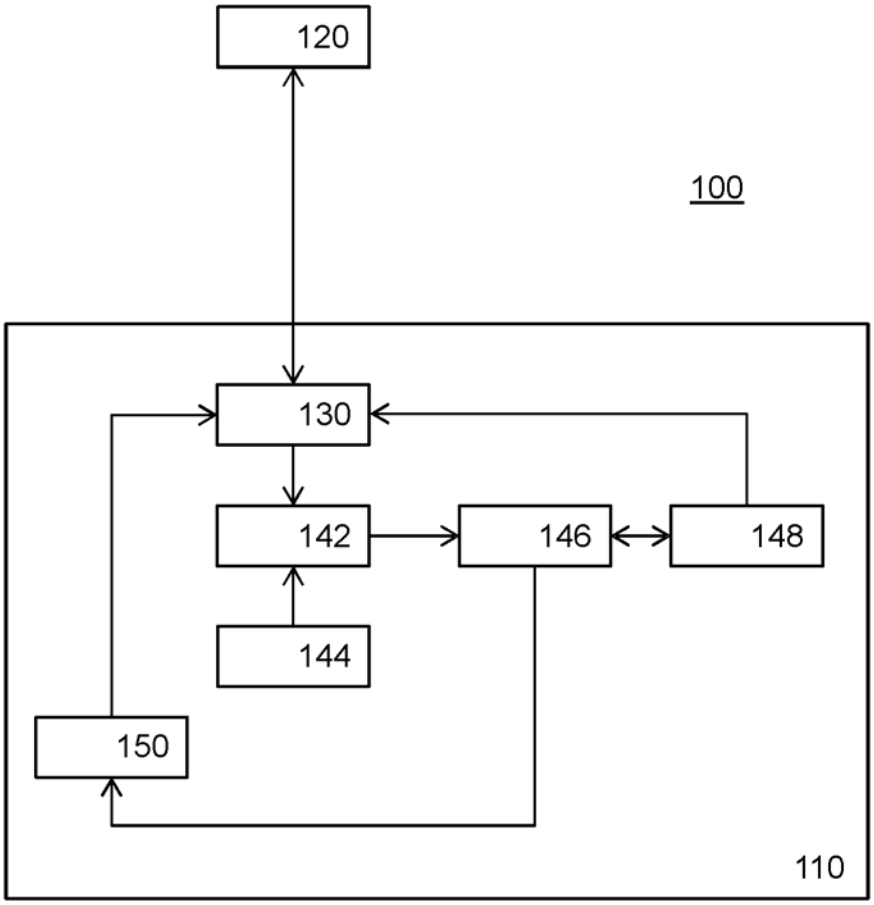


图 1b

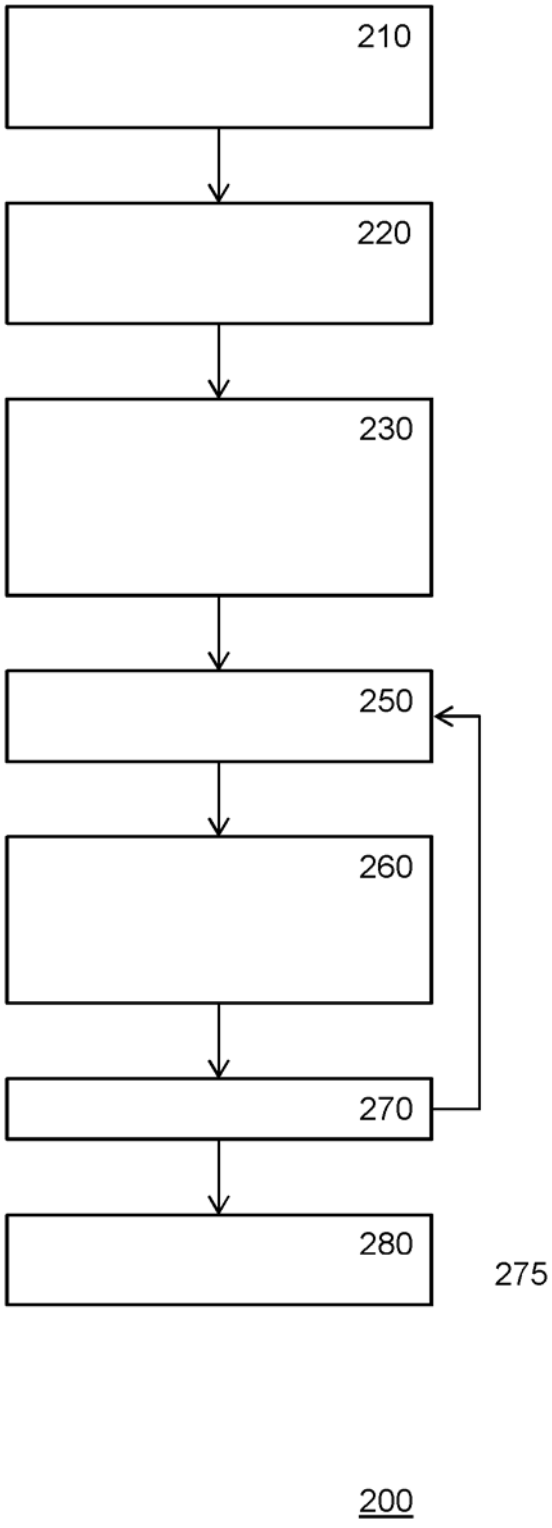


图 2

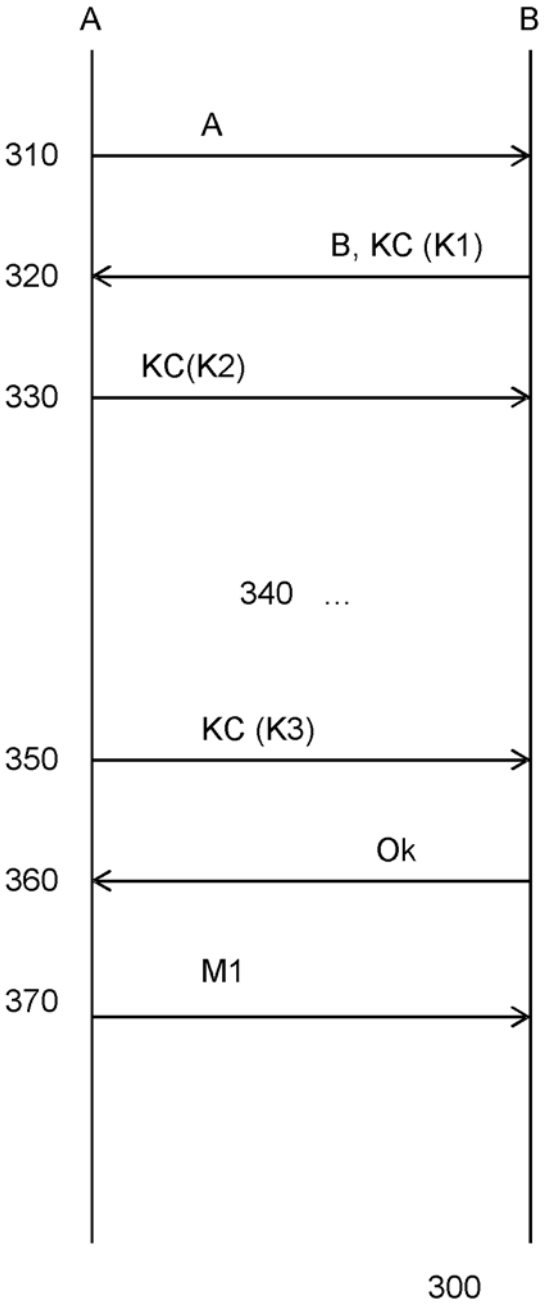


图 3

Input: b, α, η', $KM_{\eta,j}$ where $j \in \{0, \ldots, \alpha\}$
Output: $\langle(\sum_{j=0}^{\alpha} KM_{\eta,j}\eta'^{j})_N\rangle_{2^b}$

1: $N \Leftarrow 2^{(\alpha+2)b} - 1$
2: $key \Leftarrow 0$
3: **for** $j = \alpha$ **to** 0 **do**
4: $\quad key \Leftarrow \langle key \times \eta' + KM_{\eta,j}\rangle_N$
5: **end for**
6: **return** $\langle key\rangle_{2^b}$

图 4a

Input: b, α, η', $KM_{\eta,j}$ where $j \in \{0, \ldots, \alpha\}$
Output: $\langle(\sum_{j=0}^{\alpha} KM_{\eta,j}\eta'^{j})_N\rangle_{2^b}$

1: $key \Leftarrow 0$
2: **for** $j = \alpha$ **to** 0 **do**
3: $\quad temp \Leftarrow key \times \eta'$
4: $\quad R_0 \Leftarrow \langle temp\rangle_{2^{(\alpha+2)b}}$
5: $\quad R_1 \Leftarrow temp \gg (\alpha + 2)b$
6: $\quad key \Leftarrow R_0 + R_1 + KM_{\eta,j}$
7: **end for**
8: **return** $\langle key\rangle_{2^b}$

图 4b

Input: b, α, η', $KM_{\eta,j}$ where $j \in \{0, \ldots, \alpha\}$
Output: $\langle(\sum_{j=0}^{\alpha} KM_{\eta,j}\eta'^{j})_N\rangle_{2^b}$

1: $key \Leftarrow KM_{\eta,\alpha}$
2: **for** $j = \alpha - 1$ **to** 1 **do**
3: $\quad temp \Leftarrow key \times \eta' + KM_{\eta,j}$
4: $\quad R_0 \Leftarrow \langle temp\rangle_{2^{(\alpha+2)b}}$
5: $\quad R_1 \Leftarrow \langle temp \gg (\alpha + 2)b\rangle_{2^b}$
6: $\quad key \Leftarrow (R_0 + R_1)$
7: **end for**
8: $R_0 \Leftarrow \langle key\rangle_{2^b} \times \eta'$
9: $R_1 \Leftarrow \langle key \gg (\alpha + 1)b\rangle_{2^b} \times \eta'$
10: **return** $\langle R_0\rangle_{2^b} + \langle R_1 \gg b\rangle_{2^b} + \langle KM_{\eta,0}\rangle_{2^b}$

图 4c

Input: b, α, η', $KM_{\eta,j}$ where $j \in \{0, \ldots, \alpha\}$
Output: $\langle(\sum_{j=0}^{\alpha} KM_{\eta,j}\eta'^{j})_{\mathcal{N}}\rangle_{2^b}$

$key \Leftarrow KM_{\eta,\alpha}$
$red \Leftarrow 1$
for $j = \alpha - 1$ **to** 1 **do**
  $temp_{high} \Leftarrow MSB_{j+red}(key) \times \eta'$
  $temp_{low} \Leftarrow \langle LSB_1(key) \times \eta'\rangle_{2^b}$
  $temp_{high-low} \Leftarrow \langle temp_{high}\rangle_{2^{(j+red)*b}}$
  $temp_{high-low} \Leftarrow temp_{high-low} \ll ((alpha + 2 - j - red)b)$
  $temp_{high-high} \Leftarrow temp_{high} \gg ((j + red) * b)$
  $key \Leftarrow temp_{high-low} + temp_{high-high} + temp_{low} + KM_{\eta,j}$
end for
$R_0 \Leftarrow \langle key\rangle_{2^b} \times \eta'$
$R_1 \Leftarrow \langle key \gg (\alpha + 1)b\rangle_{2^b} \times \eta'$
return $\langle R_0\rangle_{2^b} + \langle R_1 \gg b\rangle_{2^b} + \langle KM_{\eta,0}\rangle_{2^b}$

图 4d

Input: b, α, η', $KM_{\eta,j}$ where $j \in \{0, \ldots, \alpha\}$
Output: $\langle(\sum_{j=0}^{\alpha} KM_{\eta,j}\eta'^{j})_{\mathcal{N}}\rangle_{2^b}$

$key \Leftarrow \langle KM_{\eta,\alpha}\rangle_{2^b}$
$temp \Leftarrow KM_{\eta,\alpha}$
for $j = \alpha - 1$ **to** 0 **do**
  $temp \Leftarrow \langle temp \gg b\rangle_{2^{(j+2)b}}$
  $temp \Leftarrow temp \times \eta' + (KM_{\eta,j} \gg (\alpha - j)b)$
  $key \Leftarrow \langle key \times \eta'\rangle_{2^b}$
  $key \Leftarrow \langle key + \langle KM_{\eta,j}\rangle_{2^b} + (temp \gg (j + 2)b)\rangle_{2^b}$
end for
return key

图 4e

$key = KM_{\alpha}$
for $j = \alpha - 1$ **to** 0 **do**
  $t \Leftarrow key \times \eta'$
  $t \Leftarrow t + (KM_j \ll b)$
  $key \Leftarrow t \gg b$
end for
return $\langle key\rangle_{2^b}$

图 4f

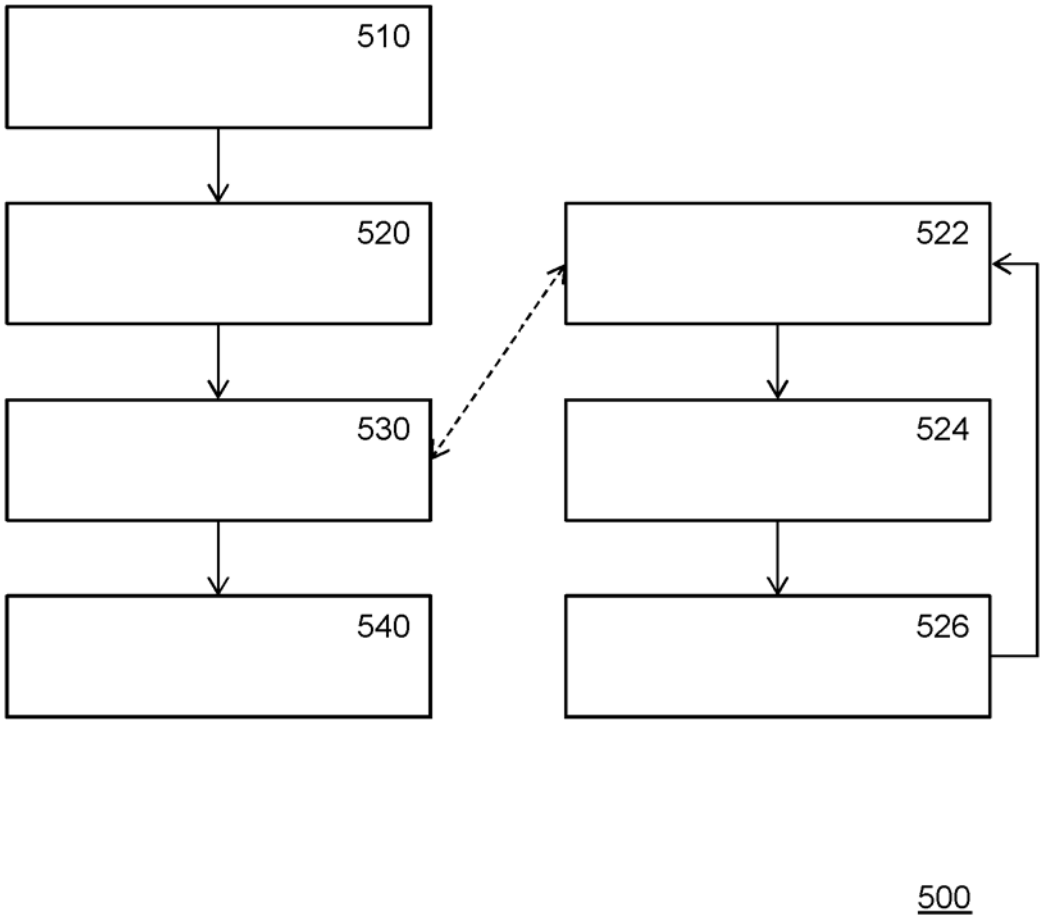


图 5