(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104854814 A
(43)申请公布日 2015.08.19

(21)申请号 201380067474.1
(22)申请日 2013.12.20
(30)优先权数据
12198794.5 2012.12.21 EP
61/740488 2012.12.21 US
(85)PCT国际申请进入国家阶段日
2015.06.23
(86)PCT国际申请的申请数据
PCT/EP2013/077842 2013.12.20
(87)PCT国际申请的公布数据
WO2014/096420 EN 2014.06.26
(71)申请人 皇家飞利浦有限公司
地址 荷兰艾恩德霍芬
(72)发明人 D. 戈梅兹 O. 加西亚莫乔恩
L.M.G.M. 托休伊泽恩
J. 古蒂尔雷兹
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 王兴秋 景军平
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)

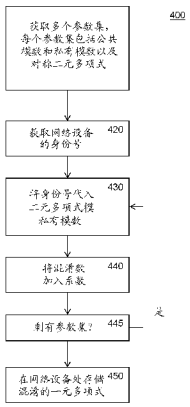
权利要求书3页 说明书23页 附图7页

(54)发明名称

密钥共享网络设备及其配置

(57)摘要

一种配置用于密钥共享的网络设备的方法，所述方法包括：以电子形式获取(410)至少两个参数集，参数集包括私有模数(p_1)、公共模数(N)和具有整数系数的二元多项式(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)的连续比特上是相同的；生成对于网络设备的本地密钥材料包括，以电子形式获取(420)对于网络设备的身份号(A)，并且对于所述至少两个参数集中的每个参数集通过以下步骤获取相应的一元多项式：使用多项式操纵设备通过将身份号代入(430)所述二元多项式来根据所述参数集的所述二元多项式确定一元多项式，并且对代入的结果模所述参数集的私有模数进行归约；以及在网络设备处电子存储(450)所生成的本地密钥材料，所生成的本地密钥材料包括每个参数集的公共模数和每个参数集的相应的一元多项式。



CN 104854814 A

1. 一种配置用于密钥共享的网络设备的方法，所述方法包括：

- 以电子形式获取（410）至少两个参数集，参数集包括私有模数（p_i）、公共模数（N）和具有整数系数的二元多项式（f_i），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）的连续比特上是相同的，

- 生成对于网络设备的本地密钥材料，所述生成步骤包括

- 以电子形式获取（420）网络设备的身份号（A），并且

- 对于每个参数集通过以下步骤来获取相应的一元多项式：使用多项式操纵设备通过将身份号代入（430）所述二元多项式中来根据所述参数集的所述二元多项式确定一元多项式并且对代入结果模所述参数集的私有模数进行归约，以及

- 在网络设备处电子地存储（450）所生成的本地密钥材料，所生成的本地密钥材料包括每个参数集的公共模数和每个参数集的相应的一元多项式。

2. 如权利要求 1 中所述的方法，其中生成网络设备的本地密钥材料包括

- 对于所述至少两个参数集中的至少两个参数集

- 生成相应于所述参数集的非零混淆多项式，

- 通过使用多项式操纵设备，将非零混淆多项式加到（440）相应于所述参数集的一元多项式，以获取混淆的一元多项式，

- 所生成的本地密钥材料包括所述混淆的一元多项式。

3. 如权利要求 2 中所述的方法，其中所述混淆多项式之和的每个系数是 2 的密钥长度次幂的倍数。

4. 如权利要求 2 中所述的方法，其中所述混淆多项式之和的每个系数除以 2 的幂，向下舍入为整数后是 2 的密钥长度次幂的倍数。

5. 如权利要求 1 或者 2 中所述的方法，其中在所有参数集中的所有二元多项式（f_i）是对称多项式。

6. 如前述权利要求中任一项所述的方法，其中在所有的参数集中，对应参数集的公共模数的二进制表示的相同的至少密钥长度（b）的连续比特与该对应的参数集的私有模数的密钥长度（b）的最低有效比特是相同的。

7. 如权利要求 6 中所述的方法，其中所述至少密钥长度（b）的连续比特是密钥长度（b）的最低有效比特。

8. 如前述权利要求中任一项中所述的配置用于密钥共享的网络设备的方法，包括

- 使用电子随机数发生器生成私有模数（p_i），和 / 或

- 使用电子随机数发生器通过生成二元多项式的一个或者多个随机系数来生成二元多项式。

9. 如前述权利要求中任一项中所述的配置用于密钥共享的网络设备的方法，其中一个或者所有公共模数满足 $2^{(a+2)b-1} \leq N$，其中 N 表示公共模数，a 表示二元多项式的次数并且 b 表示密钥长度。

10. 如前述权利要求中任一项中所述的配置用于密钥共享的网络设备的方法，其中至少两个参数集至少包括多个私有模数（p_i）和具有系数模 p_i 的多个二元多项式（f_i），使得存在密钥长度（b）的一组连续位置，其中公共模数的二进制表示与所有私有模数的二进制表

示相一致，所述方法进一步包括：

确定一元多项式包括，将身份号代入所述多个二元多项式（f_i）的每一个二元多项式中，归约模相应于所述一个对称二元多项式的所述多个私有模数中的私有模数，并且将多个归约的多个结果相加。

11. 如前述权利要求中任一项中所述的配置用于密钥共享的网络设备的方法，其中生成混淆数以使得$|\epsilon_{i,k}^{A}| < 2^{(a+2-k)b-2}$，其中$\epsilon_{A,i}$表示混淆数，i 表示相应于系数的单项式的次数，a 表示二元多项式的次数并且 b 表示密钥长度。

12. 一种用于第一网络设备确定共享密钥的方法，所述密钥是密码学密钥，所述方法包括

- 以电子形式获取第一网络设备的本地密钥材料，所述本地密钥材料包括至少两个一元多项式和相应的公共模数，
- 获取（510）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，
- 对于所述至少两个一元多项式中的每个而言，将第二网络设备的身份号代入（530）所述一元多项式中，并且对代入结果模相应于所述一元多项式的公共模数进行归约，并且
- 将归约模公共模数的结果加到一起，并且归约（540）模密钥模数，并且
- 根据归约模密钥模数的结果导出（550）共享密钥。

13. 如权利要求 11 中所述的用于第一网络设备确定共享密钥的方法，包括

- 确定（560,570）第一网络设备和第二网络设备是否已经导出相同的共享密钥，并且如果没有，则根据归约模密钥模数的结果导出另外的共享密钥。

14. 如权利要求 12 或者 13 中所述的方法，包括将代入结果模公共模数除以零比特串除数并且将除的结果向下舍入为整数，所述零比特串除数是 2 的幂，所述零比特串除数大于 1。

15. 一种被配置成确定共享密钥的网络设备，所述密钥是密码学密钥，所述网络设备包括

- 本地密钥材料获取器 344，其被配置成以电子形式获取网络设备的本地密钥材料，所述本地密钥材料包括至少两个一元多项式和相应的公共模数，
- 接收器（330），其被配置成获取不同的另外的网络设备的身份号
- 多项式操纵设备 342，其被配置成对于所述至少两个一元多项式中的每个而言，将第二网络设备的身份号代入（530）所述一元多项式中，并且对代入结果模相对应于所述一元多项式的公共模数进行归约，并且将归约模公共模数的结果加到一起，并且归约（540）模密钥模数，以及
- 密钥导出设备 346，其被配置成根据归约模密钥模数的结果导出（550）共享密钥。

16. 一种用于配置用于密钥共享的网络设备的系统，所述系统包括

- 密钥材料获取器（100），其用于以电子形式获取至少两个参数集，参数集包括私有模数（p_1）、公共模数（N）和具有整数系数的二元多项式（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）的连续比特上是相同的，
- 发生器（200），其用于生成对于网络设备的本地密钥材料，所述发生器包括
- 网络设备管理器（250），其用于以电子形式获取网络设备的身份号（A）和用于在网络设备处电子地存储所生成的本地密钥材料，

- 多项式操纵设备(240),其被配置成对于每个参数集,通过以下步骤来获取相应的一元多项式:通过将身份号代入(430)所述二元多项式中来根据所述参数集的所述二元多项式确定一元多项式,并且对代入结果模所述参数集的私有模数进行归约。

17. 一种计算机程序,其可选地在计算机可读介质上体现,所述计算机程序包括计算机程序代码模块,所述计算机程序代码模块被适配成当所述计算机程序在计算机上运行时执行如权利要求 1 至 14 中的任一项的所有步骤。

密钥共享网络设备及其配置

技术领域

[0001] 本发明涉及一种配置用于密钥共享的网络设备的方法，该方法包括生成对于该网络设备的本地密钥材料，其包括以电子形式获取对于该网络设备的身份号，使用多项式操纵设备通过将身份号代入二元多项式来根据该二元多项式确定一元多项式，并且在该网络设备处电子地存储所生成的本地密钥材料。

[0002] 本发明进一步涉及一种用于第一网络设备确定共享密钥的方法，所述密钥是密码学密钥，所述方法包括：以电子形式获取对于第一网络设备的本地密钥材料，所述本地密钥材料包括一元多项式；获取对于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；将第二网络设备的身份号代入该一元多项式并且据此导出共享密钥。

[0003] 本发明进一步涉及用于配置用于密钥共享的网络设备的系统和被配置成确定共享密钥的网络设备。

背景技术

[0004] SONG GUO 等人的文章：“用于在传感器网络中建立成对密钥的基于置换的多元多项式方案(A Permutation-Based Multi-Polynomial Scheme for Pairwise Key Establishment in Sensor Network)”，COMMUNICATIONS(ICC)，2010 IEEE INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ(新泽西)，美国，2010 年 5 月 23 日(2010-05-23)，第 1-5 页中公开了现有技术的解决方案。

[0005] 考虑包括多个网络设备的通信网络，在这样的网络设备对之间设立安全连接是个问题。解决该问题的一种方式在 C. Blundo、A. De Santis、A. Herzberg、S. Kutten、U. Vaccaro 和 M. Yung 的“用于动态会议的极度安全的密钥分发(Perfectly-Secure Key distribution for Dynamic Conferences)”，Springer Lecture Notes in Mathematics，卷 740，第 471-486 页，1993 年(被称为“Blundo”)中描述。

[0006] 假设中央机构(也被称为网络机构或者可信第三方(TTP))生成对称二元多项式 f(x,y)，其具有在含有 p 个元素的有限域 F 中的系数，其中 p 是质数或者是质数的幂。每个设备具有在 F 中的身份号，并且由 TTP 向每个设备提供本地密钥材料。对于具有标识符 η 的设备，本地密钥材料是多项式 f(η,y) 的系数。

[0007] 如果设备 η 希望与设备 η’通信，则它使用它的密钥材料来生成密钥 K(η, η’) = f(η, η’)。因为 f 是对称的，所以生成相同的密钥。

[0008] 如果攻击者知道 t+1 或者更多设备的密钥材料，则这种密钥共享方案的问题出现，其中 t 是二元多项式的次数。攻击者可以随后重建多项式 f(x,y)。此时，系统的安全性被完全破坏了。考虑任何两个设备的身份号，攻击者可以重建在该对设备之间共享的密钥。

发明内容

[0009] 具有一种用于建立两个网络设备之间的共享密钥的改进方法将是有利的。本发明由独立权利要求限定；从属权利要求限定有利的实施例。提供了一种配置用于密钥共享的

网络设备的方法和一种用于使网络设备确定所共享的密钥的方法。

[0010] 配置用于密钥共享的网络设备的方法包括以电子形式获取至少两个参数集，参数集包括私有模数(modulus)、公共模数和具有整数系数的二元多项式，公共模数的二进制表示和私有模数的二进制表示至少在密钥长度连续比特上是相同，生成对于网络设备的本地密钥材料包括，以电子形式获取对于网络设备的身份号并且对于所述至少两个参数集中的每个参数集通过以下步骤来获取相对应的一元多项式：使用多项式操纵设备通过将身份号代入所述二元多项式来根据该参数集的二元多项式确定一元多项式并且对代入的结果模(modulo)该参数集的私有模数进行归约(reduction)，以及在网络设备处电子存储所生成的本地密钥材料，所生成的本地密钥材料包括每个参数集的公共模数和每个参数集的相对应的一元多项式。

[0011] 用于第一网络设备确定共享密钥(所述密钥是密码学密钥)的方法包括：以电子形式获取对于第一网络设备的本地密钥材料，所述本地密钥材料包括至少两个可选地混淆一元多项式和相对应的公共模数，获取对于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，对于所述至少两个可选混淆一元多项式中的每个而言：将第二网络设备的身份号代入所述一元多项式中，对代入的结果模相应于所述一元多项式的公共模数进行归约，将归约模公共模数的结果加到一起，对模密钥模数进行归约，以及根据归约模所述密钥模数的结果来导出共享密钥。

[0012] 在实施例中，所述方法包括对代入结果模公共模数进行归约，将结果除以 2 的幂并且归约模密钥模数。

[0013] 多个网络设备中的任何两个网络设备的对能够采用很少资源来协商共享密钥，所述多个网络设备中的每个网络设备具有身份号和针对该身份号生成的本地密钥材料。两个网络设备仅需要交换它们的身份号(这不需要被保密)并且执行多项式计算。计算的类型无需要求大的计算资源，这意味着该方法适合于低成本、高容量类型的应用。

[0014] 已经从根密钥材料中的共同多项式中获取了本地密钥材料；这允许一对网络设备中的两个网络设备获取相同的共享密钥。如果所有的二元多项式都是对称的，那么任何两个网络设备都可以导出共同的多项式。如果一些或者所有二元多项式是不对称的，则一些设备对可以导出共享密钥，而一些对则不能导出共享密钥。

[0015] 从参数集中(特别是从多个不同公共模数和多个二元多项式中)导出本地密钥材料。所产生的本地密钥材料包括多个、典型不同的一元多项式，每个一元多项式具有相对应的公共模数。

[0016] 如果使用了仅仅一个参数集，那么网络设备被提供有多项式的系数，使得通过估计该多项式模 N 并且取 b 比特，该网络设备能够生成与任何其他设备的 b 比特密钥。这关于所谓的噪声多项式插值问题，即，通过具有那些 b 比特密钥中的许多 b 比特密钥，攻击者可能能够恢复给定的、受攻击的实体的多项式。

[0017] 例如，面向单个参数集系统的攻击可以通过以下 2 个步骤来得到那些 b 比特值：攻击者损害与 N_c 密钥材料相关联的 N_c 设备，并且攻击者使用那些 N_c 密钥材料来获取 N_c 的 b 比特密钥(通过以受攻击的设备的标识符来估计每个密钥材料)。这意味着对于噪声多项式插值问题做出的进展可以扩展至对于单个参数集系统的攻击。这被认为是不合期望的。

[0018] 具有多个参数集，通过在设备上以及在本地密钥生成期间混合模操作来避免这个问题。

[0019] 在一对设备 A 和 B 之间共享的共同密钥 K_{AB} 作为至少两个（一般地，m’ 个）子密钥 K_{AB}^{i} 的加法（即，$K_{AB} = K_{AB}^{1} + K_{AB}^{2}$）而被获取。每个子密钥 K_{AB}^{i} 根据不同密钥材料（其中，通过以公共模数 N_i 为模执行模操作）而生成。因为在本地密钥生成期间以及在共享密钥生成期间混合模操作，所以不可能将噪声多项式插值攻击扩展到密码系统。即使攻击者能够得到 N_c 的 b 比特密钥，每个 N_c 的 b 比特密钥也是从两个子密钥中导出的，每个子密钥来自不同密钥材料的估计。但是攻击者将不能区分子密钥，使得攻击者不能恢复受攻击的设备的这两个（一般是 m’ 个）密钥材料。

[0020] 存在对于设备的攻击的两种级别的严重性。在较低的严重性中，攻击者仅仅能够得到许多共同的共享密钥。在较高的严重性中，攻击者能够得到许多本地密钥材料。其结果是，在网络设备处混合模操作是针对较低严重性的攻击的很好的对抗手段。然而，如果攻击者有权访问密钥材料本身，那么他也有权访问子密钥。

[0021] 通过向设备的两个密钥材料加入噪声来避免后者的问题。向本地密钥材料加入混淆数干扰了在本地密钥材料和根密钥材料之间的关系。将存在于未被混淆的一元多项式和（对称的）二元多项式之间的关系将不再存在。这意味着对于这样的方案，直接的攻击不再起作用。

[0022] 有趣的是，通过向设备的两个密钥材料加入噪声以使得噪声的相加等于零模 2^b，进一步改进了系统。在该情况下：所生成的密钥依然是有噪声的，因此，攻击者不能使用它们来恢复受攻击的设备的密钥材料共享；而为了移除噪声，攻击者必须加它们，但是随后他具有如上文的加后的值，并且不能在源自每个密钥材料的分量之间进行区分。这种技术可以容易地推广到任何数量的密钥材料。条件也可以被扩展，以确保噪声等于并不位于最低有效比特而是位于其他位置的 b 比特中的零。

[0023] 在实施例中，每个参数集中的所有公共模数的二进制表示和私有模数的二进制表示至少在密钥长度（b）的连续比特上是相同的。注意，可以使用多个私有模数，可以选取这些私有模数以使得公共模数的多个私有模数中的任一个的二进制表示和该私有模数的二进制表示至少在密钥长度（b）的连续比特上是相同的。对于所述多个私有模数 a 的每个私有模数而言，选取具有整数系数的可选地对称的二元多项式，以获取多个并且可选地对称的二元多项式。

[0024] 因为本地密钥材料的导出使用不同于公共模数的私有模数，所以在比如单个有限域中起作用时将存在的数学关系被干扰。这意味着用于分析多项式的常规数学工具（例如，有限代数）不再适用。攻击者最多可以使用少得多的有效结构，诸如格子（lattice）。此外，当导出共享密钥时，在常规的数学意义上不兼容的两个模操作被组合；所以在两个地方避免了数学结构。该方法允许直接的成对密钥的生成并且对于捕获极大量的网络设备（例如，10^5 级别的或者甚至更多）是有弹性的。另一方面，因为私有模式和公共模数在若干连续比特上重叠，所以具有本地密钥材料的两个网络设备很可能能够导出相同的共享密钥。

[0025] 本发明人特别意识到，公共模数不需要是质数。在实施例中，公共模数是合成的。同样，没有理由公共模数在其二进制表示中应该是“全一”的比特数，例如仅仅由“1”的比特组成的数。在实施例中，公共模数不是 2 的幂减去 1。在实施例中，公共模数的二进制表

示包括至少一个零比特(不算第一位的零,即,公共模数的二进制表示包括低于该公共模数的最高有效比特的至少一个零比特)。在实施例中,公共模数是 2 的幂减 1 并且是合成的。

[0026] 在实施例中,一个或者多个参数集的公共模数大于一个或者多个私有模数。

[0027] 在实施例中,公共模数减私有模数的二进制表示的至少密钥长度的连续比特是全零的比特。这个差应该通过使用公共模数减私有模数的符号数表示来估计,而不是使用补码表示(two-complement representation)。可替换地,可以要求公共模数减私有模数的绝对值的二进制表示的至少密钥长度的连续比特是全零的比特。存在这样的一组密钥长度(b)的连续位置,其中,公共模数的二进制表示与所有私有模数的二进制表示相一致。

[0028] 公共模数与私有模数相一致的连续比特位置可以是最低有效比特。在实施例中,公共模数减私有模数的二进制表示的密钥长度的最低有效的比特是全零的比特;这具有如下优点,当导出共享密钥时,不需要除以 2 的幂。

[0029] 在实施例中,在所有参数集中,对应参数集的公共模数的二进制表示的相同的至少密钥长度(b)的连续比特与该对应的参数集的私有模数的密钥长度(b)的最低有效的比特相同。也就是说,存在一组连续比特位置,其表明,在每个参数集中,公共模数和私有模数在哪里相一致。虽然这组连续比特位置对于所有的参数集是相同的,但是这些比特本身可以在不同参数集上是不同的。在实施例中,至少密钥长度(b)的连续比特是密钥长度(b)的最低有效的比特。也就是说,这组比特位置是最低有效的比特位置。

[0030] 允许的是,多个私有模数中的一个私有模数等于公共模数。然而,如果使用了仅仅一个私有模数,那么这是不合期望的。

[0031] 期望的是,私有模数引入充分的非线性。在实施例中,存在公共模数不同于每个私有模数的一组连续比特位置。此外,还可以强制的是,私有模数在它们自身中是不同的;私有模数的二进制表示的成对比较还可以在比如至少密钥长度的一组连续比特中的至少一个比特上是不同的,该组对于所有私有模数是相等的,并且可能地,对于公共模数也是相同的。

[0032] 网络设备可以是装配有电子通信和计算模块的电子设备。网络设备可以例如以 RFID 标签的形式附接到任何非电子物体。例如,这种方法可以适用于“物联网”。例如,物体(特别是低成本的物体)可以装配有无线电标签,它们可以通过该无线电标签进行通信(例如,可以被标识)。可以通过诸如计算机之类的电子模块为这样的物体编制清单。被偷盗或者损坏的物品可以被容易地跟踪和定位。一种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灯。这样的灯可以安全地传送它的状态;这样的灯可以被安全地控制,例如被打开和 / 或关闭。网络设备可以是多个网络设备中的一个,每个网络设备包括用于发送和接收身份号和用于发送电子状态消息的电子通信器,并且每个网络设备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。

[0033] 在实施例中,在本发明中的方法可以被用作用于安全性协议(诸如 IPSec、(D)TLS、HIP 或者 ZigBee)的密码学方法。特别地,使用这些协议中的一种协议的设备与标识符相关联。想要与第一设备通信的第二设备可以采用第一设备给出的它的标识符来生成共同的成对密钥,并且该成对密钥(或者凭借例如密钥导出函数据此导出的密钥)可以而被用在以上基于预先共享的密钥的协议的方法中。特别地,如在本发明中所定义的设备的标识符可以是网络地址,诸如 ZigBee 短地址、IP 地址或者主机标识符。标识符还可以是设备的 IEEE

地址或者与设备相关联的专用比特串，使得设备在制造期间接收与 IEEE 地址相关联的一些本地密钥材料。

[0034] 导出共享密钥可以用于许多应用。典型地，共享密钥将是密码学的对称密钥。对称密钥可以用于机密，例如，传出的或者传入的消息可以用对称密钥来加密。只有有权访问两个身份号和这两个本地密钥材料之一（或者有权访问根密钥材料）的设备将能够对通信进行解密。对称密钥可以用于认证，例如，传出或传入的消息可以用对称密钥来认证。以这种方式，可以验证消息的来源。只有有权访问两个身份号和这两个本地密钥材料之一（或者有权访问根密钥材料）的设备将能够创建被认证的消息。

[0035] 配置用于密钥共享的网络设备的方法将典型地由网络机构（例如，可信的第三方）来执行。网络机构可以从另一个源获取所需要的材料（例如根密钥材料），但也可以自己生成这种材料。例如，可以生成公共模数。例如，即使公共模数是系统参数并且被接收，也可以生成私有模数。

[0036] 在实施例中，选取公共模数 N 的一个或者多个或者所有公共模数以使得其满足 $2^{(a+2)b-1} \leq N \leq 2^{(a+2)b} - 1$，其中，a 表示二元多项式的次数，b 表示密钥长度。例如，在实施例中，$N = 2^{(a+2)b} - 1$。针对后一选择的模操作可以被特别高效地实施。

[0037] 具有固定的公共模数具有以下优点，即：它不需要被传送到网络设备，而是可以与例如它们的系统软件集成在一起。特别地，可以通过使用随机数发生器来选取公共模数。

[0038] 公共模数和私有模数可以被表示为比特串。它们还可以各自使用特定数学结构而被缩写。例如，替代存储私有模数，也可以存储它与公共模数的差，这会短得多。

[0039] 以公共模数减私有模数的二进制表示的“密钥长度”数量的最低有效比特是全零的比特的这样的方式来选取私有模数，这增大了在一对网络设备中的第一网络设备处的共享密钥与在该对网络设备中的第二网络设备处所导出的共享密钥相近的可能性；也就是说，私有模数的二进制表示在“密钥长度”的最低有效位置中具有与公共模数的二进制表示相同的比特。例如，如果密钥长度是 64，则可以通过从公共模数中减去 2^64 的倍数来选取私有密钥。在实施例中，公共模数减去私有模数再除以 2 的密钥长度次幂小于 2 的密钥长度次幂。

[0040] 在实施例中，以电子形式获取或者生成多个私有模数，对于多个私有模数中的每个私有模数，选取具有整数系数的对称二元多项式，以获取多个对称的二元多项式，以使得对称的二元多项式相对应于每个私有模数。确定一元多项式包括，将身份号代入多个对称的二元多项式中的每一个中，针对模所述多个私有模数中相应于该对称的二元多项式的私有模数进行归约，并且将多个归约的多个结果加在一起。对于不同模数具有多个对称二元多项式增大了安全性，因为不兼容的结构被进一步混合。典型地，私有模数是不同的。如果相应的代数结构非常不同的话，则具有多个私有模数进一步使得分析甚至更加复杂；例如，将它们选取为互质的，特别是成对地互质的，甚至更特别地，将它们选取为相异的质数。

[0041] 具有不同的私有模数并且特别是多个私有模数将使得攻击者的分析复杂化。为了进一步增强安全性，对于系数的附加控制是可能的。在实施例中，将多个归约所产生的多个一元多项式加到一起的机构验证每个所产生的系数的数值是否过小或者过大，例如，小于最小阈值或者在最大阈值以上。这甚至进一步地提高了安全性，因为在这两种情况的任一种情况下，攻击者可能会找出多个归约的分量，如果它们过大或者过小的话。例如，如果在

相加后产生的系数值等于 1 并且仅存在两个一元多项式，那么攻击者知道，要么与第一多项式相关联的相应系数是 1 而与第二多项式相关联的系数是 0，要么情况相反。特别地，生成针对设备的本地密钥材料的机构可以验证本地密钥材料的每个所产生的系数的值是否至少是“最小值”并且至多是“最大值”。这种检查可以被省略，特别是在公共模数相对接近于所有私有模数并且密钥材料的所有元素都在 0 与 N-1 之间的情况下。如果 TTP 能够指派身份号，则如果 TTP 检测到大或者小的系数，那么它也可以向设备指派另一个身份号。

[0042] 在实施例中，每个特定私有模数使得公共模数减该特定私有模数的二进制表示的密钥长度（b）的最低有效比特是全零的比特。

[0043] 公共模数既可以比私有模数大，也可以比私有模数小。在实施例中，公共模数减私有模数的二进制表示具有至少密钥长度的全零的比特。至少密钥长度的零比特中的零比特是连续的，并且可以存在于该二进制表示中的任一点处。在公共模数和私有模数之间的差中具有为零比特的串避免了混淆进位太过分。注意，该串可以但不需要存在于所有参数集中。

[0044] 在实施例中，存在整数参数“s”以使得公共模数减私有模数再除以 2 的 s 次幂后的密钥长度的最低有效比特是全零的。参数“s”对于所有私有模数是相同的，但是可以对于每个参数集是不同的。

[0045] 例如，可以定义作为 2 的幂的零比特串除数，从而，每个特定私有模数使得公共模数减该特定私有模数再除以该零比特串除数后的二进制表示的密钥长度（b）的比特是全零的比特。如果最低有效比特是零，则可以将该零比特串除数取为 1。在实施例中，该零比特串除数大于 1。考虑到与沿着最低有效比特方向对比特移位的结果相同的结果，除以 2 的幂将被解释为整数除法。忽略除法的任何余数。

[0046] 为了生成密钥长度比特的共享密钥，网络设备首先应用附加的除法步骤。第一网络设备如下估计密钥材料：第二设备的身份号模每个参数集的公共模数并且将结果相加，然后除以 2^s 并且对模 2 的密钥长度次幂进行归约。注意，这等同于首先在公共模之后应用模数 2^(s+ 密钥长度），并且然后除以 2^s。此处，“除以”包括向下舍入。

[0047] 在实施例中，使用随机数发生器来生成私有模数。在实施例中，生成多个私有模数使得它们是成对互质的。例如，多个私有模数可以迭代地生成，从而对每个新的私有模数验证它们依然是成对互质的，并且如果不是，则丢弃最后生成的私有模数。实施例包括，使用随机数发生器迭代地生成候选模数，以使得公共模数减该候选模数后的二进制表示的密钥长度（b）的连续比特是全零的比特（例如，密钥长度的最低有效比特），直到通过使用素数测试设备，该候选模数满足素数测试为止，其中如此获取的、满足素数测试的候选模数被用作私有模数。素数测试可以例如是 Miller-Rabin 素数测试或者 Solovay-Strassen 素数测试。

[0048] 次数为 a 的、以 x 和 y 作为变量的对称二元多项式仅具有形式为 $x^i y^j$ 的单项式，其中 $i \leqslant a$，$j \leqslant a$。此外，相应于 $x^i y^j$ 的系数与 $x^j y^i$ 的系数相同。这可以用来将所存储的系数数量减少大约一半。注意，使用更宽松的次数定义。将单项式的次数定义为单项式中的变量的最大次数。所以 $x^j y^i$ 的次数是 max(i,j)，即，$i \leqslant a$，$j \leqslant a$。所以，例如，我们称为次数为 1 的多项式具有一般形式 a+bx+cy+dxy，（注意，因为仅仅考虑对称多项式，所以得到 b=c）。注意，如果期望的话，可以对二元多项式施加附加的限制，包括例如仅使用满足

i+j ≤ a 的单项式，但是这不是必需的。

[0049] 在实施例中，对称二元多项式由网络机构生成。例如，对称二元多项式可以是随机的对称二元多项式。例如，可以使用随机数发生器来将系数选为随机数。

[0050] 虽然所使用的混淆很大地增大了对于攻击的弹性，特别是对于其中多个本地密钥材料被组合的共谋攻击的弹性，但是它具有潜在的缺陷。有时，由第一网络设备所导出的共享密钥的所有比特并非与由第二网络设备所导出的共享密钥的所有比特完全相同。这主要是因为在混淆系数加入之后进位的比特的误匹配导致的。另一个原因是缺少如下效果，即：在密钥生成期间的影响所生成的进位比特的每个私有模数的模效果。虽然麻烦，但是这个缺陷可以以各种方式来解决。通过更小心地选取混淆，差异的可能性，并且特别是很大差异的可能性可以被显著地减小。此外，发现的是，差异(如果存在的话)很可能位于所生成的密钥的最低有效比特中。所以通过移除最低有效比特中的一个比特或者多个比特，可以增大完全相同的共享密钥的可能性。例如，在确定共享密钥的方法的实施例中，其包括确定第一网络设备和第二网络设备是否导出了相同的共享密钥，并且如果没有，则根据对模密钥模数进行归约的结果来导出另外的共享密钥。可以导出另外的共享密钥，直到发现两侧都相等为止。如果在共享密钥中保持有低于阈值数量的比特，则方法可以终止。对于一些应用而言，仅仅可以接受的是，一定百分比的网络设备不能进行通信。例如，在消息可以沿着各种路径路由的移动自组网无线网络中，如果一些网络设备不能通信，则不存在连通性的损失。

[0051] 在实施例中，移除了共享密钥的若干最低有效比特；例如，所移除的比特数量可以是 1、2 或者更多、4 或者更多、8 或者更多、16 或者更多、32 或者更多、64 或者更多。通过移除更多的最低有效比特，具有不相等的密钥的几率降低了；特别是，其可以被降低到任何期望的阈值。共享密钥相等的几率可以通过遵循数学关系来计算，其也可通过实验来确定。

[0052] 此外，可以控制混淆数的选择，在实施例中，对于相应于较高次数的单项式的系数而言，从其选取混淆数的范围减小。特别地，可以要求 $|\epsilon_{A,i}| < 2^{(a+1-i)b}$，其中 $\epsilon_{A,i}$ 表示对于第 i 个单项式的混淆数，i 表示相应于系数的单项式的次数，a 表示二元多项式的次数并且 b 表示密钥长度。A 表示为其生成本地密钥材料的网络设备。在实施例中，为每个系数生成混淆数(例如通过使用以上公式)。可以对不同的网络设备应用不同的混淆。例如，即使存在 3 个或者更多个网络设备，那么对于每个网络设备，也可以生成不同的混淆数。

[0053] 注意，混淆数可以被限制为正数，但是这不是必需的，混淆数可以是负的。在实施例中，通过使用随机数发生器生成混淆数。多个混淆数可以被生成并且与一元多项式的系数相加以获取混淆的一元多项式。一元多项式中的一个或者多个(优选地，甚至所有)系数可以以这种方式而被混淆。

[0054] 网络设备的身份号中的比特数量通常被选取为小于或者等于密钥长度。身份号可以是比特串，比如 32 或者 64 或者更长的比特串。密钥长度可以是 32 或者更长、48 或者更长、64 或者更长、96 或者更长、128 或者更长、256 或者更长。密钥长度可以被选取为要更长几个比特，以便减少所确定的共享密钥的相应的最低有效比特的数量。另一方面，在实施例中，身份号的长度长于密钥长度。在该情况下，模操作的效果可以对所生成的密钥的密钥长度的比特的最低有效比特产生更大的效果，以使得对于希望生成共同密钥的一对设备而言，那些比特可以不相等。然而，具有更长的标识符长度可以在安全性上产生积极的效果，因为在进行相应的计算时，更多的比特被混合在一起。

[0055] 多项式操纵设备可以被实施在计算机上(比如在集成电路上)运行的软件中。多项式操纵设备可以在硬件中非常高效地实施。组合也是可能的。例如,多项式操纵设备可以通过操纵表示多项式的系数阵列来实施。

[0056] 在网络设备处电子地存储所生成的本地密钥材料可以通过以下步骤实施:例如使用有线连接或者使用无线连接向网络设备电子地发送所生成的本地密钥材料,并且将所生成的本地密钥材料存储在网络设备处。这可以在网络设备中的集成电路的制造或者安装期间(例如在测试期间)完成。测试设施可以包括或者连接到网络机构。这也可以在设备成功加入到操作网络中之后(即,在网络访问或者引导程序之后)发生。特别地,本地密钥材料可以作为操作网络参数的一部分而分发。

[0057] 以电子形式获取对于第一网络设备的本地密钥材料可以通过从用于配置用于密钥共享的网络设备的系统(例如,网络机构设备)电子地接收本地密钥材料而完成。获取本地密钥材料还可以通过从本地存储装置(例如,诸如闪速存储器之类的存储器)取回本地密钥材料来完成。

[0058] 获取对于第二网络设备的身份号可以通过从第二网络设备(例如,直接从第二网络设备)接收身份号来完成,例如,从第二网络设备无线地接收身份号来完成。

[0059] 公共模数和密钥模数可以被存储在网络设备中。还可以从网络机构接收它们。它们还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。归约模这样的密钥模数可以通过丢弃除了密钥长度的最低有效比特之外的所有比特来完成。首先,代入的结果被归约模公共模数,其随后进一步被归约模密钥模数。

[0060] 虽然不要求,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,应避免的是,密钥模数除尽公共模数,因为那时归约模公共模数就可以被略去。

[0061] 用于两个设备之间的密钥一致的方法可以使用若干二元多项式作为根密钥材料。可以通过使用 x- 变元的多项式作为根密钥材料来使用该用于密钥一致的方法,以用于 x 方之间的 x- 一致。在这种扩展中,可信的第三方估算在相应的环中的变量中的 x- 变元的多项式,所产生的 x-1 个变元的多项式随后相加在整数上,从而生成存储在设备上的本地密钥材料。当 x 个设备需要在密钥上一致时,设备以另外 x-1 个设备的标识符来估算其本地密钥材料。

[0062] 将不对称的二元多项式用作根密钥材料(即,f(x,y)!=f(y,x))允许适应两组设备的构建,诸如在第一组中的设备接收 KM(Id,y) 和在第二组中的设备接收 KM(x,iD) 作为存储在设备上的 KM 本地密钥材料。属于相同分组的两个设备不能生成共同密钥,但是在不同分组中的两个设备可以。进一步参见 Blundo。

[0063] 网络设备的身份号可以被计算为含有与设备相关联的信息的比特串的单向函数。单向函数可以是密码学的哈希函数,诸如 SHA2 或者 SHA3。单向函数的输出可以被截短,以使得其适合于标识符的大小。可替换地,单向函数的大小小于最大标识符大小。

[0064] 在实施例中,对称多项式涉及形式为$\langle ax^i y^i \rangle_{p_j}$的单个单项式,其中$<>_p$表示模操作。在该情况下,元素在有限组内,并且操作是乘法。公共模数可大于私有模数或者小于私有模数,如果存在多个稀有模数,一些公共模数可以大于私有模数并且一些公共模数

可以小于私有模数。

[0065] 根密钥材料可以在任何环中进行估算。可能的是，使用单个单项式(诸如Ax^a)的多项式，在该情况下，可以使用一组。

[0066] 本发明的一个方面涉及用于配置用于密钥共享的网络设备的系统(例如，网络机构)，该系统包括用于以电子形式获取至少两个参数集的密钥材料获取器，参数集包括私有模数、公共模数和具有整数系数的二元多项式，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的连续比特上是相同的；用于生成对于网络设备的本地密钥材料的发生器包括用于以电子形式获取网络设备的身份号并用于在网络设备处电子地存储所生成的本地密钥材料的网络设备管理器和多项式操纵设备，发生器被配置成，对于所述至少两个参数集中的每个参数集，通过使用多项式操纵设备通过将身份号代入所述二元多项式来根据该参数集的二元多项式确定一元多项式并且对代入结果模该参数集的私有模数进行归约，来获取相应的一元多项式，以及在网络设备处电子存储所生成的本地密钥材料，所生成的本地密钥材料包括每个参数集的公共模数和每个参数集的相应的一元多项式。

[0067] 该系统的实施例包括用于生成混淆数的混淆数发生器，例如随机数发生器，多项式操纵设备被配置用于将混淆数加到一元多项式的系数中，以获取混淆的一元多项式，所生成的本地密钥材料包括混淆的一元多项式。混淆数可以被表示为混淆多项式的系数。在实施例中，混淆多项式之和的每个系数是 2 的密钥长度次幂的倍数。在实施例中，混淆多项式之和的每个系数除以 2 的幂是 2 的密钥长度次幂的倍数。除以 2 的幂可以通过向下舍入来计算。

[0068] 本发明的一个方面涉及被配置成确定共享密钥的第一网络设备，所述密钥是密码学密钥，第一网络设备包括：用于以电子的形式获取对于第一网络设备的本地密钥材料的本地密钥材料获取器，所述本地密钥材料包括至少两个一元多项式(可选地，混淆一元多项式)和相应的公共模数；用于获取对于第二网络设备的身份号的接收器，第二网络设备与第一网络设备不同；多项式操纵设备，其用于：对于所述至少两个可选地混淆的一元多项式中的每个而言，将第二网络设备的身份号代入所述一元多项式中，并且对代入结果模相应于所述一元多项式的公共模数进行归约，以及将归约模公共模数的结果加到一起并且归约模密钥模数；以及用于根据归约模密钥模数的结果来导出共享密钥的密钥导出设备。

[0069] 密钥导出设备可以被实施为计算机(例如，集成电路)、为运行的软件、在硬件中、在两者的组合中等，其被配置用于根据归约模密钥模数的结果导出共享密钥。

[0070] 根据归约模密钥模数的结果导出共享密钥可以包括，应用密钥导出函数，例如在开放移动联盟(Open Mobile Alliance)的 OMA DRM 规范(OMA-TS-DRM-DRM-V2_0_2-20080723-A，章节 7.1.2 KDF)中定义的函数 KDF 和相似的函数。导出共享密钥可以包括丢弃一个或者多个最低有效比特(在应用密钥导出函数之前)。导出共享密钥可以包括加入、减去、或者串接整数(在应用密钥导出函数之前)。

[0071] 多个网络设备(每个网络设备具有身份号和相应的本地密钥材料)可以一起形成通信网络，该通信网络被配置用于保护例如网络设备对之间的机密和 / 或被认证的通信。

[0072] 密钥生成是基于 ID 的，并且允许在设备对之间生成成对的密钥。第一设备 A 可以依赖于根据本地密钥材料和身份号导出密钥的算法。

[0073] 在实施例中，第一网络设备向第二网络设备发送密钥确认消息。例如，确认消息

可以包括消息的加密，以及可选地消息本身。第二网络设备可以验证该消息的加密。消息可以被固定并且存在于第二设备处，以避免需要发送它。消息可以是随机的或者一次性数(nonce)等等，在该情况下，其可以与加密一起发送消息。第二设备可以用消息进行回复，该消息含有密钥是否一致的指示。第二设备还可以以其自身的密钥确认消息来回复。如果第一和/或第二设备发现密钥不相等，则它们可以例如通过删除最低有效比特等等来启动密钥均衡过程。

[0074] 网络设备和系统可以是电子设备。网络设备可以是移动网络设备。

[0075] 根据本发明的方法可以作为计算机实施的方式实施在计算机上或者在专用硬件中或者在两者的组合中。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存储在计算机可读介质上的非暂时性程序代码模块，其用于当所述程序产品在计算机上执行时，执行根据本发明的方法。

[0076] 在优选的实施例中，计算机程序包括计算机程序代码模块，其被适配成当计算机程序在计算机上运行时执行根据本发明的方法的所有步骤。优选地，计算机程序体现在计算机可读介质上。

附图说明

[0077] 本发明的这些和其他方面根据下文描述的实施例而显而易见，并且将参考下文描述的实施例进行阐述。在图中，

图 1 是图示出根密钥材料发生器的示意性方框图，

图 2 是图示出本地密钥材料发生器的示意性方框图，

图 3 是图示出通信网络的示意性方框图，

图 4 是图示出生成本地密钥材料的示意性流程图，

图 5 是图示出生成所共享的密钥的示意性流程图，

图 6 是图示出生成所共享的密钥的示意性顺序图。

[0078] 应该注意的是，在不同的图中具有相同的附图标记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。在这样的项目的功能和/或结构已经被解释的情况下，在具体实施方式中对其进行重复解释是不必要的。

具体实施方式

[0079] 虽然本发明容许许多不同形式的实施例，但是在附图中示出并且将在本文中详细地描述一个或者多个特定实施例，其中应理解，本公开内容被认为是本发明的原理的示例，而不意图将本发明限制为所示出和所描述的特定实施例。

[0080] 以下描述了密钥共享方法的实施例。该方法具有设立阶段和使用阶段。设立阶段可以包括发起步骤和注册步骤。发起步骤不涉及网络设备。

[0081] 发起步骤选择系统参数。发起步骤可以由可信的第三方(TTP)执行。然而，系统参数也仍然可以被认为是作为输入而给出的。在该情况下，可信的第三方不需要生成它们，并且发起步骤可以被跳过。例如，可信的第三方可以从设备制造商接收系统参数。设备制造商可能已经执行了发起步骤以获取系统参数。为了阐述的方便，将认为由可信的第三方

执行发起步骤，注意，这不是必需的。

[0082] 在发起步骤中，建立了若干参数集。考虑到网络设备的标识号，参数集用来生成本地密钥材料；从每个参数集中获取一元多项式和相对应的公共模数。向网络设备给出本地密钥材料，但是不向网络设备给出对于参数集的访问。因为参数集允许人们生成新的本地密钥材料，所以参数集仅对于可信方是已知的，并且对一般网络设备保密。

[0083] 网络设备 A 可以从其本地密钥材料和不同的设备 B 的标识号生成共享密钥。为了做到这一点，网络设备 A 使用其本地密钥材料执行计算。

[0084] 发起步骤

在发起步骤中，选择根密钥材料。有些参数是全局参数。

[0085] 选择将在使用阶段中在设备之间所共享的密钥的期望的密钥长度；这个密钥长度被称为“b”。用于低安全性应用的典型值可以是 64 或者 80。用于消费者级别的安全性的典型值可以是 128。高度秘密的应用可能更倾向于 256 或者甚至更高的数值。在算法的安全性强度和 b 之间不需要存在直接的关系；所提供的安全性将至多是 b。取决于未来用于攻击系统的算法，算法的安全性可以低于 b。

[0086] 选择将生成的参数集数量；参数集的数量被称为“t”。t 的高数值暗示着攻击所产生的系统(例如，使用基于格子(lattice)的技术)是更难的。另一方面，t 的较高数值还暗示着在网络设备处的较大的计算和存储需要。对于非常低的安全性的应用，t=1 的数值是可能的，然而，它可能暗示着，给定足够数量的暴露(compromised)密钥，底层密钥材料可以被恢复。推荐的是，至少采用 t=2 的数值；这个数值已经使得所需要的密码分析的复杂度(例如，基于格子的攻击)显著增大。然而，对于高安全性应用而言，可以使用 3、4 或者甚至更高的数值。

[0087] 接下来，选择数量为 t 的参数集。对于 $j = 1, \cdots, t$，每个参数集 j 包括期望的次数 a、公共模数 N、至少一个私有模数 p_1 和至少一个对称二元多项式 f_1。在方便时，该公共模数将用下标来标注，以指示该公共模数 N_j 所属的参数集。

[0088] 在下文中讨论选择这些参数的有利方式。特别地，每个参数集的二元多项式是安全性敏感的，并且将不对一般网络设备公开；也没有理由公开私有模数，所以推荐的是，保守这些秘密，认识到这些甚至可以减少对系统的攻击。在网络设备处需要密钥长度 b 和公共模数 N_j，并且所述密钥长度 b 和公共模数 N_j 不能对可信方保密。

[0089] 每个参数集都有助于底层难解问题的难解度。如将在下文中解释的，对于参数的一些选择将导致比其他选择更难解的问题。原则上，参数集的选择是独立的，例如，人们可以选取选择具有相应于较高安全性的数值的一个参数集，并且选择具有较小参数的第二集合。在该情况下，第二和 / 或另外的集合主要有助于避免对于难解集合的攻击。对于这个情形，可能稍微更容易的是，导出在安全性上的界限。另一方面，人们还可以选择难度相当的所有参数集。在后一情况下，问题的难度来自于所有集合。这最优化了网络设备处的计算资源。

[0090] 参数集选择步骤

这些步骤将被重复 t 次；每一次针对一个期望的参数集。

[0091] 选择期望的次数；该次数控制某些多项式的次数。次数将被称为“a”，其至少为 1。对于 a 的实际选择是 2。更安全的应用可以使用更大的 a 值，比如 3 或 4，或者甚至更大。对

于简单的应用而言，a=1 也是可能的。a=1 的情况与所谓的“隐藏数问题”有关；更大的“a”值与确认这些情况难以破解的噪声多项式插值问题有关。

[0092] 选择多项式数量。多项式的数量将被称为“m”。对于 m 的实际选择是 2。更安全的应用可以使用更大的 m 值，比如 3 或 4，或者甚至更大。应注意，低复杂度的应用可以施加小的 m 值，因为大数值 m 暗示着在 TTP 处的更高的实施方式的复杂度。

[0093] 安全性参数 a 和 m 的较大数值增加了系统的复杂度，并且相应地增大了其难处理性。越复杂的系统越难以分析，因而对于密码分析越有抵抗力。方便地，次数 a 可以对于所有参数集是相同的，同样，m 可以对于所有参数集是相同的；注意，这不是必需的。

[0094] 在实施例中，选择满足 $2^{(a+2)b-1} \leq N$ 并且最优选地还满足 $N \leq 2^{(a+2)b}-1$ 的公共模数 N。界限不是严格必需的；系统也可以使用更小 / 更大的 N 值，但这不被认为是最佳选项。

[0095] 通常，密钥长度、多项式的次数和数量将例如由系统设计者预先确定，并且作为输入提供给可信方。作为实际的选择，人们可以采用 $N=2^{(a+2)b}-1$。例如，如果 a=1、b=64，那么 N 可以是 $N=2^{192}-1$。例如，如果 a=2、b=128，那么 N 可以是 $N=2^{512}-1$。为 N 选取上述间隔的上界或者下界具有容易计算的优点。为了增大对于攻击者的复杂度，人们可以选择在针对 N 的范围内的随机数。

[0096] 由可信的第三方（TTP）选择数量为 m 的私有模数 $p_1, p_2, \cdots, p_m$。模数是正整数。在注册步骤期间，每个设备将与身份号相关联。每个所选择的私有模数大于所使用的最大身份号。例如，人们可以通过要求身份号小于或者等于 2^b-1 以及所选择的私有模数大于 2^b-1 来约束身份号。每个所选择的数满足以下关系 $p_j=N+\gamma_j \cdot 2^b$。其中 γ_j 是使得 $|\gamma_j| < 2^b$ 的整数。选择满足这个要求的数的一种实际方法是选取 m 个随机整数 γ_j 的集合使得 $-2^b+1 \leq \gamma_j \leq 2^b-1$，并且根据关系 $p_j=N+\gamma_j \cdot 2^b$ 计算所选择的私有模数。可以允许使 $|\gamma_j|$ 更大一点，然而，可能会出现问题，因为模操作太过分的话，所共享的密钥可能不相等。

[0097] 对于 m>1，系统更加复杂，并且因此更加安全，因为针对不同模数的模操作被组合，即使这样的操作在常规的数学意义上不是兼容的。出于这个原因，有利的是，选取所选择的私有模数作为成对的差。

[0098] 生成数量为 m 的、次数为 a_j 的对称二元多项式 $f_1, f_2, \cdots f_m$。所有的次数满足 $a_j \leq a$，最优选为 $a = MAX\{a_1, \ldots, a_m\}$。实际的选择是对每个多项式采用次数 a。二元多项式是具有两个变量的多项式。对称多项式 f 满足 f(x,y)=f(y,x)。每个多项式 f_j 在由整数模 p_j 形成的有限环中被估计，并通过计算模 p_j 而被获取。整数模 p_j 形成具有 p_j 个元素的有限环。在实施例中，多项式 f_j 以从 0 到 p_j-1 的系数来表示。二元多项式可以被随机选择（例如通过选择在这些界限内的随机系数）。

[0099] 密钥共享的安全性取决于这些二元多项式，因为它们是系统的根密钥材料；所以优选地，采取强力的措施来保护它们，例如控制过程、防篡改的设备等等。优选地，所选择的整数 $p_1, p_2, \cdots p_m$ 也是保密的，包括相对应于 p_j 的值 γ_j，但是这不那么重要。还将以以下形式来指代该二元多项式：对于 j=1,2,...,m，写为 $f_j(x,y) = \sum_{i=0}^{a} f_{i,j}(x) y^i$。

[0100] 以上实施例可以以若干方式变化。可以以多种方式来选取对于公共和私有模数的

限制，以使得一元多项式的混淆是可能的，而在网络设备处获取的共享密钥足够经常地彼此保持足够紧密。如所解释的，什么样才是足够的将取决于应用、所要求的安全性级别和在网络设备处可用的计算资源。以上实施例将正整数相组合，以使得在生成多项式部分时实行的模操作在它们相加在整数上时以非线性的方式组合，从而创建用于存储在网络设备上的本地密钥材料的非线性结构。以上对于 N 和 p_j 的选择具有如下属性，即：(i)N 的大小对于所有网络设备是固定的，并且与 a 相联系；(ii) 非线性效果表现在形成存储在设备上的密钥材料的系数的最高有效比特上。因为这种特定形式，所以所共享的密钥可以通过在归约模 N 之后归约模数 2^b 而生成。

[0101] 这些设计构思可以以更一般的方式被应用，从而对上一段中提到的方面(i)和(ii)进行改进。在下文中给出用于选取公共模数和私有模数的不同的一般构造。为了解决第一点(i)，对于 N 和 p_j，这种结构适合更一般化的表达，其中，写为 $p_j = 2^X + \gamma_j 2^{Y_j} - 1$，以使得对于每个 j，$Y_j + b\alpha_j = X \text{ and } |\gamma_j| < 2^b$。这种表达允许更多变化形式的 p_j，同时在引入非线性效果时确保最大效果。注意，也可以使得 $Y_j + b\alpha_j \approx X$，其中左手侧与右手侧之间的差是密钥长度的零点几。

[0102] 为了解决第二点，上文中对于 N 和 p_j 的形式适合甚至更一般化的表达，其中 $p_j = \beta 2^X + \gamma_j 2^{Y_j} + \zeta_j 2^{Z_j}$。通过设定例如 $\zeta_j = -1, \beta = 1$ 和 $Z_j = 0 \ \forall j$，得到之前的表达，其中不同的 γ_j 值在存储在网络设备上的密钥材料的系数的最高有效比特中引入了非线性效果。在该情况下，常数公共模数(N)是 $N = 2^X - 1$，而在模操作中所涉及的不同正整数的生成中使用的私有变量部分是 $\gamma_j 2^{Y_j}$。可替换地，可以设定 γ_j =1，β =1，Z_j=0，Y_j=(α $_j$+1)b，X=(α $_j$+2)b $\forall j$，而 ζ_j 对于不同 j 是不同的，以使得 $|\zeta_j| < 2^b$。在该情况下，ζ_j 上的差允许在存储在节点上的本地密钥材料的系数的最低有效比特中引入非线性效果。在该情况下，公共部分的构造也是不同的并且等于 $N = \beta_j 2^{X_j} + \gamma_j 2^{Y_j} = 2^X + 2^{b(\alpha_j+1)}$，即，该部分保持恒定。注意，在该情况下，非线性效果在最小部分中，并且由于针对上文提到的最大混合效果的条件，所以在 $Y_j - Z_j - \log_2(\zeta_j)$ 之间的差于是必须是 $\alpha_j b$。以相似的方式，可以遵循相同的概念来定义其他构造。

[0103] 如上文示出的，对于参数的许多选择是可能的。然而，一些选择将给出更好的实施方式。特别地，公共模数的选择是重要的。例如，对于公共模数的一些选择允许有效的模操作。此外，优选地，公共模数对于从中得到密钥的比特(比如 LSB)的效果是不同的。不同的效果可以通过以下步骤来测试：执行用于生成共享密钥的操作并且测试 p_j 的差异是否导致生成密钥的不同方式。这可以在下文的示例中观察到。

[0104] 例如，有利的是，选择在密钥长度数量的最低有效比特上具有小差异(比如小于预定差异)的公共模数。例如，一个实施例可以使用诸如 t=2，和 N_1=$2^{(a+2)b}$-1 和 $N_2 = 2^{(a+2)b} - 2 - 1$ 之类的数。在这个特定情况下，项 -2 在密钥生成阶段起到重要作用，因

为归约模数 N_1 将不包括该效果，但是归约模数 N_2 将包括该效果。注意，在该情况下，归约涉及将高于(a+2)b 比特的溢出比特移到最低部分。

[0105] 然而，以该方式选取公共模数的问题在于，仅仅远小于 2^b 的有限数量的选项是可用的。一般地，希望在 N 中引入 2^h 项，以使得 h<b 并且 h>1。问题还在于，实际上受不同形式的 N 影响的比特数量将大约是 b-h 并且将仅仅存在 2^h 左右个不同数字。为了克服这些问题，例如，具有对于 N 的更多选项并且使可以用于被不同操作影响的密钥的比特数量最大化，可以按以上两段的方式使用 p_i 的更一般化的定义。在该情况下，非线性效果被引入到多项式系数的 MSB 和 LSB 两者中，这例如是通过使用 $p_i = N - \gamma_i 2^{b(a+1)} - \zeta_i$ 以及相应的公共模数 $N = 2^{(a+2)b} - 2^{ba}$。如此处定义的，对于所有的 p_i 而言，γ_i 和 ζ_i 被选取为不同的，并且优选地，对于所有参数集而言，也被选取为不同的。在该情况下，密钥从中间比特生成，而不是从 LSB 生成。

[0106] 在下文中是相似的选择。在这些等式中，第一索引 i 标引参数集并且最大为 t；第二索引 j 标引每个参数集所使用的数 p 的数量，并且最大为 m。

$$N_i = 2^{(a+2)b} - 2^{ba} - \zeta_i$$

$$p_{i,j} = N_i - \gamma_{i,j} 2^{b(a+1)}$$

[0107] 实际的选择是取 t=2。随后，可选取每个参数集。对于每个参数集，实际的选择是取 m=2。尤其在正上方的等式中，这些是好的选择。采用这种构造，可以通过变化 b- 比特的 ζ 值(比如随机地变化)来找到许多 N_i。在这种构造中，$\gamma_{i,j}$ 参数在生成存储在设备上的密钥材料部分中执行混合。这可以由可信方完成。ζ 参数执行设备上的密钥混合。最优选地，在该情况下，还加入噪声，其遵循与实施例中相同的动机。在该情况下，对于噪声的条件需要被更新，以使得噪声之和(即，混淆多项式)在从中(即，从中间比特)提取密钥的位置处等于零。

[0108] 优选地，公共模数(比如 N_1 和 N_2) 不全是 2^b 的倍数。那么这是因为对于正整数 a、m、n 和对于适当的整数 q，有 $a = qmn + \langle a \rangle_{mn}$，并且所以 $a \equiv \langle a \rangle_{mn} \bmod n$，从其中，推断出 $\langle a \rangle_n = \langle \langle a \rangle_{mn} \rangle_n$。因此，如果 N_1 和 N_2 两者都是 2^b 的倍数，那么 $\langle \langle F_\eta^1(\eta') \rangle_{N_1} + \langle F_\eta^2(\eta') \rangle_{N_2} \rangle_{2^b} = \langle F_\eta^1(\eta') + F_\eta^2(\eta') \rangle_{2^b}$。也就是说，问题归约为 t=1 的情况。

[0109] 注册步骤

在注册步骤中，每个网络设备被指派密钥材料(KM)。网络设备与身份号相关联。身份号可以是例如由 TTP 按要求指派的或者可以已经被存储在设备中(例如，在制造时存储在设备中)等等。

[0110] TTP 通过按照下式计算 t 个多项式来生成针对具有身份号 A 的设备的一组密钥材料 KM^A：

$$F_i^A(X) = \sum_{j=1}^{m} < f_j(x, A) >_{p_j} + \sum_{k=0}^{a} \epsilon_{i,k}^A X^k = \sum_k C_{i,k}^A X^k \text{。}$$

[0111] 在正上方的等式中，索引 i 标引参数集，即，范围从 1 到 t。索引 j 标引每个参数集中的多项式的数量和私有模数的数量。索引 k 标引混淆多项式中的系数。注意，为每个参数集选择一个混淆多项式。一些或者所有参数集可以不具有混淆多项式。此外，来自相应于以上的一元多项式的参数集的公共模数被包括在本地密钥材料中。

[0112] X 是形式变量。注意，密钥材料是非线性的。符号 $<\cdots>_{p_j}$ 表示对括号之间的多项式的每个系数进行归约模 P_j。符号“$\epsilon_{A,i}$”表示随机整数，其是混淆数的示例，使得 $|\epsilon_{i,k}^{A}| < 2^{(a+2-k)b-2}$。注意，随机整数中的任一个可以是正的或者负的。对每个设备，再次生成随机数 ϵ。因此，项 $\sum_{k=0}^{a} \epsilon_{i,k}^{A} X^k$ 表示对于每个 i 的次数 a 的 X 的多项式，其系数长度随着次数增大而变小。可替换地，更一般化但是更复杂的条件是 $\sum_{k=0}^{a} |\epsilon_{i,k}^{A}| \cdot 2^{b+k}$ 是小的，例如 <2a。

[0113] 所有其他附加内容可使用自然整数算法，或(优选地)它们使用附加的模 N_i。所以，一元多项式 $\sum_{j=1}^{m} < f_j(x,A) >_{p_j}$ 的估计是通过模较小模数 p_j 而各自独立完成，但是这些归约的一元多项式它们自己之和优选地通过模 N 来完成。此外，加入混淆多项式 $\sum_{k=0}^{a} \epsilon_{i,k}^{A} X^k$ 可以通过使用常见整数算法或者优选地使用模 N 来完成。密钥材料包括系数 $C_{i,k}^{A}$ 其中，k=0,…,a 和 i=1,…,t。密钥材料可以被呈现为如上文的一组多项式。在实践中，密钥材料可以被存储为整数 $C_{i,k}^{A}$ 的列表，例如二维阵列。设备 A 还接收数 N_i 和 b。对多项式的操纵可以被实施为例如对含有系数的阵列的操纵，该阵列例如以预定的次序列出了所有系数。注意，多项式可以以其他数据结构来实施，例如实施为包括(次数、系数)对的集合的关联阵列(又叫做“映射”)，优选地使得每个系数最多在集合中出现一次。向设备提供的系数 C_i^A 优选地处于范围 0,1,…,N-1 内。由于标识符大小是小的，可能发生的是，系数中的并非所有比特都将用于密钥的生成。在该情况下，需要存储仅仅相关的系数部分。

[0114] 如在本文档开始处指示的，为了降低设备 A 导出与其配对设备 B 不同的共享密钥的可能性，可以选择混淆多项式以使得对于每个 k=0,…,a 有

$$\sum_{i=1}^{t} \varepsilon_{i,k} \equiv 0 \bmod 2^b$$

也就是说，所有混淆多项式之和是 2^b 的倍数。如已经提到的，这具有良好的性质，即：如果攻击者想要通过添加密钥材料移除噪声，那么他将混合通过用不同的模数执行模操作而获取的密钥材料。如果他不添加它们的话，那么密钥材料被噪声所隐藏。

[0115] 如果使用对于 N 的更一般的构造和整数 p_j，则需要适配混淆多项式以使得随机数 ϵ 影响系数的不同部分。例如，如果非线性效果被引入到存储在网络设备上的密钥材料的系数的最低有效比特中，那么随机数应该仅仅影响系数的最高部分和系数的最低部分中的可变数量的比特。这是上文描述的方法的直接扩展，并且其他扩展是可行的。

[0116] 使用阶段

一旦两个设备 A 和 B 具有身份号并且已经从 TTP 接收了他们的密钥材料，它们就可以使用其密钥材料来获取共享密钥。设备 A 可以执行以下步骤来获取它的共享密钥。首先，设备 A 获取设备 B 的身份号 B，随后 A 通过计算下式来生成共享密钥，即：

$$K_{AB} = < \Sigma_i \ < F_i^A(X)|_{X=B} >_{N_i} >_{2^b} = < \Sigma_i \ < \Sigma_k \ C_{i,k}^A B^k >_{N_i} >_{2^b}$$

也就是说，针对值 B，A 根据其密钥材料估计其每一个一元多项式 F_i^A；估计密钥材料的结果是整数。接下来，设备 A 首先对估计的结果模相应的公共模数 N_i 进行归约。接下来，将模估计之后的所有多项式 F_i^A 的估计的结果相加为整数，并且随后将这个总和的结果进行模密钥模数 2^b。结果将被称为 A 的共享密钥，它是在 0 到 $2^b - 1$ 范围内的整数。对设备 B 部分而言，设备 B 可以通过如下与 A 相同的方式来生成 B 的共享密钥，即：针对身份 A 估计其密钥材料并且对结果模 N 进行归约，随后模 2^b。

[0117] 鉴于上文的描述，如果使用 N 和正整数 p_j 的更一般化的表达，那么用于获取 b- 比特密钥的方法需要进行小的适配。特别地，可以对私有模数取 $p_{i*m+j} = \beta 2^X + \gamma_{i*m+j} 2^{Y_{i,j}} + \delta 2^W + \zeta_i 2^{Z_i}$，而对公共模数取 $N_i = \beta 2^X + \delta 2^W + \zeta_i 2^{Z_i}$，于是这允许凭借 b- 比特项 γ_{i*m+j} 在密钥材料部分中引入非线性。注意，在该特定构造中，在每个密钥材料集中具有 m 个多项式并且这些多项式中的每个多项式由标识符 j 来标引。此外，可以具有凭借 i 标引的最多 t 个不同的密钥材料集。还应注意，典型地，$Y_{i,j}$ 是常数，其中 $\forall i,j$。此外，对于 i=1，…，t 的不同 N_i，b- 比特项 ζ_i 是不同的，并且当混合从节点上的不同密钥材料生成的密钥时，ζ_i 是引入非线性效果的项。在该情况下，密钥如下生成：

$$K_{AB} = < \frac{\Sigma_i \ < F_i^A(X)|_{X=B} >_{N_i}}{2^W} >_{2^b}$$

如可见的，t 个密钥材料部分中的每个密钥材料部分以 x=B 进行估计并且通过模数 N_i 进行归约。在这个归约中，ζ_i 的效果被引入。因为对于所有 p_{i*m+j} 共同的、2 的最小幂是 w，那么结果除以 2^w（整数除法）使得共同密钥可以被生成。

[0118] 因为在根密钥材料中的二元多项式是对称的，所以 A 的共享密钥和 B 的共享密钥通常是相等的，但是并非必然总是相等的。对于参数集中的私有模数（整数 $p_1, p_2, \ldots, p_m$）和对于随机数 ϵ 的特定要求使得密钥通常是相等的，并且通过 2 的密钥长度次幂，其几乎总是彼此相近。如果 A 和 B 已经获取了相同的共享密钥，那么它们可以使用该共享密钥作为在 A 和 B 之间共享的对称密钥；例如，其可以被用于各种各样的密码学应用，例如，它们可以交换使用共享密钥加密和 / 或认证的一个或者多个消息。优选地，密钥导出算法被应用于共享密钥，以便进一步保护主密钥，例如，可以应用哈希函数。

[0119] 如果 A 和 B 没有获取到相同的共享密钥，那么几乎确定的是，通过移除密钥的若干最低有效比特，这些密钥是彼此相近的，所生成的密钥可以几乎总是被弄得相同。A 和 B 可以通过执行密钥确认来验证它们共享的密钥是否是相等的，例如，A 可以向 B 发送含有对 (m，E(m)) 的消息，其中 m 是消息（比如固定字符串或者随机数），并且 E(m) 是使用 A 的共享密钥的加密。

[0120] 通过使用 B 的共享密钥解密 E(m)，B 可以验证密钥是否是相等的。如果是，B 可以通过通知 A 这种情景来响应于 A。

[0121] 如果密钥不相等，则 A 和 B 可以参与到密钥均衡协议中。例如，它们可以利用两个密钥在算法上彼此相近的事实。例如，网络设备 A 和 B 可以迭代地移除最低有效比特并且发送密钥确认消息，直到密钥相等为止。在获取到相等的密钥之后，A 和 B 可以执行密钥导出算法来重新获得常见密钥长度的密钥。

[0122] 优选地，所选择的 m 个私有模数$p_1, p_2, \ldots, p_m$是成对互质的。如果这些数是成对互质的，则增大了在模操作之间的兼容性的缺失。获取成对互质的数可以通过以下步骤获取到：按次序选择整数，针对每个新的整数，测试不同数的所有对是否依然是互质的，如果不是互质的，则从集合中移除刚刚选择的数。这个过程继续，直到所有的 m 个数都被选择为止。

[0123] 通过要求所选择的 m 个私有模数$p_1, p_2, \ldots, p_m$是不同的质数，复杂度甚至进一步地增大。在该情况下，可以要求每个质数具有形式$p_j = N + \gamma_j \cdot 2^b$。其中，$\gamma_j$是使得$|\gamma_j| < 2^b$的整数。实验已经确认，这些质数是可容易地得到的。例如，可以重复地选择随机数γ_j并且测试所得到的 p_j，直到发现质数。如果应用如上文描述的更一般化的表达，这些同样适用。实际上，它遵循用于等差数列(arithmetic progression)的质数定理，即：只要 a 与 b 具有大约相同的数量级，特别是对于 a<b，则这样的质数是充足的。特别地，对于在组 64、128、196、256 中的密钥长度和在组 2、3 中的次数的任何组合而言，通过实验确认了这种形式的许多质数可以通过使用上文的算法在实际的时间限制内生成。当使用质数时，每个多项式 f_j由此取自具有 p_j个元素的有限域中。

[0124] 用于选取在注册和使用阶段期间使用的各种参数的许多变型是可能的。例如，在简化的实施例中，私有模数小于公共模数，并且满足关系$p_j = N - \beta_j \cdot 2^b$，其中$\beta_j$是使得$\beta_j < 2^b$的正整数。选择满足这种要求的数的一种实际方法是选取一组 m 个的随机正整数β_j使得$\beta_j < 2^b$，并且根据关系$p_j = N - \beta_j \cdot 2^b$计算所选择的私有模数。

[0125] 如所记载的，在$\gamma_j - z_j - \log_2(\zeta_j)$之间的差可以是$\alpha_j b$。以相似的方式，可以遵循相同的理念来定义其他构造。特别地，可以对私有模数写出$p_j = \beta 2^x + \gamma_j 2^{\gamma_j} + \delta 2^w + \zeta_j 2^{z_j}$并对公共模数写出$N = \beta 2^x + \delta 2^w$。这种构造的特定实例化是$p_j = 2^{2(a+1)b} + \gamma_j 2^{(a+1)b} + 2^{ab} + \zeta_j$和$N = 2^{2(a+1)b} + 2^{ab}$。在该情况下，项$\gamma_j$和$\beta_j$的绝对值小于 2^b并且负责对设备上的本地存储的密钥材料的系数的 MSB 和 LSB 创建非线性效果。注意，因为设备标识符大约是 b 个比特长，所以γ_j (β_j)影响在整数模 p_j的环中所估计的多项式部分的系数的 MSB（LSB）。然后，在生成对于设备的本地密钥材料期间，在不同环中的多项式部分的系数被相加在整数上，以使得贡献的起源被掩盖。

[0126] 密钥可以如下生成，即：$K_{AB} = < \frac{\sum_i < F_i^A(X) | X=B > N_i}{2^W} >_{2^b}$，但是如果使用了允许对

MSB 和 LSB 两者都引入非线性效果的、p_j和 N 的甚至更一般化的表达，那么在归约模 N 之后除以 2 的 W 次幂，其中 2^W是 2 的最高整数次幂，其中 N 是整数倍数。N 和 p_j的其他构造可能需要除以 2 的另外的幂次。因为在根密钥材料中的二元多项式是对称的，所以 A 的共享密钥和 B 的共享密钥通常是(但不必然总是)相等的。

[0127] 图 1 是图示出根密钥材料发生器 100 的示意性框图。密钥材料获取器被配置成提供除了身份号之外的被本地密钥材料发生器需要用于生成本地密钥材料的输入数据。密钥发生器是密钥材料获取器的示例。替代生成输入数据的全部或者一部分，一些参数还可以通过由根密钥材料发生器通过接收它们而获取到；例如密钥获取器可以包括用于接收输入数据(例如，公共和私有模数)的电子接收器。密钥材料获取器从外部源获取除了身份号之外的所有需要的参数。在一个实施例中，a、b、m 是预定的(例如，接收的)，参数集中的公共模数和私有模数和相应的(对称的)二元多项式是生成的。在实施例中，公共模数也是预定的(例如，接收的)。

[0128] 根密钥发生器 100 生成多个参数集并且包括数量为 t 的参数集元件 130，其含有需要被生成的参数集数量。例如，t=2 或者 t=3 等等。

[0129] 根密钥发生器 100 包括多项式次数元件 112、密钥长度元件 114 和多项式数量元件 116，其被配置成，对于给定的参数集，分别提供多项式次数、密钥长度和多项式数量，即，a、b 和 m。典型地，密钥长度元件 114 将对于所有的参数集都是相同的。典型地，多项式次数元件 112 也将对于所有的参数集是相同的，但是这不是必需的。在一些实施例中，多项式数量元件 116 跨参数集而变化；例如，一些参数集可以使用 m=1，而一些参数集可以使用 m=2。跨所有集合，使 m 为常数(比如 m=1 或者 m=2)也是可能的。

[0130] 虽然这些元件可以例如视情况而生成，但是典型地，这些参数由系统设计者选取。例如，元件可以被设计为非易失性存储器，或者被设计为用于接收元素值的接收器，或者被设计为连接到接收器的易失性存储器等等。适当的选择包括 t=2、a=2、b=128、m=2。任一数字可以增大或者减小，以获取更安全或者不那么安全的系统。

[0131] 根密钥发生器 100 包括被配置成提供参数集的公共模数 N 的公共模数元件 110。公共模数可以或者可以不由系统设计者所选取。例如，公共模数可以被设定为允许快速归约的方便的数(接近或者等于幂次二)。在由元件 112 和 114 确定的范围内选取公共模数。

[0132] 根密钥发生器 100 包括被配置成提供私有模数 p 或者多个私有模数$p_1,\ldots,p_m$的私有模数管理器 122。例如，它们在适当的界限内被随机地选取。

[0133] 根密钥发生器 100 包括对称二元多项式管理器 124，其被配置成提供对称二元多项式 f 或者多个对称二元多项式$f_1,\ldots,f_m$。为每个对称二元多项式选取模相应的私有模数(即，具有相同索引的私有模数)的随机系数。系数可以在范围 0 到 p-1 之内选取，并且可以被随机地选取。

[0134] 私有模数可以通过向公共模数加入或者从其减去 2 的密钥长度次幂的倍数来选取。这将导致生成与公共模数的差以一连串连续的零结尾的私有模数。还可以选取公共模数和一个或者多个私有模数使得一连串的密钥长度的连续的零不出现在结尾处，而是出现在另一个位置，比如从最低有效比特开始计数的位置“s”。

[0135] 图 1’示出了由根密钥发生器 100 生成的根密钥材料 180 的示例。根密钥材料 180 包括参数集数量 140，在该情况下，它具有值 3。根密钥材料 180 包括三个参数集。第一集

合包括公共模数 141、私有模数 151、153 和 155 以及相应的二元多项式 152、154、156。第二集合包括公共模数 142、私有模数 161 和 163 以及相应的二元多项式 162 和 164。第三集合包括公共模数 143、私有模数 171、173 和 175 以及相应的二元多项式 172、174 和 176。在该情况下，多项式的次数隐含在多项式的表示中，也可以使其是明显的。在根密钥材料 180 的这个示例中，密钥长度 144 也被记录。

[0136] 在操作期间，根密钥材料获取器 100 重复生成参数集，直到已经产生的集合的数量等于元件 130 中的数。参数集的数量可以被记录在根密钥材料 180 中的 140 处。

[0137] 图 2 是图示出本地密钥材料发生器 200 的示意性框图。密钥材料发生器 100 和本地密钥材料发生器 200 一起形成用于配置用于密钥共享的网络设备的系统。

[0138] 本地密钥材料发生器 200 包括多项式操纵设备 240。本地密钥材料发生器 200 包括根密钥材料元件 210，其用于向多项式操纵设备 240 提供根密钥材料（即，向多项式操纵设备 240 提供多个参数集）、进而以便于产生多个一元多项式。元件 210 可以由密钥材料发生器 100 的相应元件实施；这些元件还可以是连接到密钥材料发生器 100 的存储器或者总线。

[0139] 本地密钥材料发生器 200 包括用于向多项式操纵设备 240 提供混淆数“$\epsilon_{A,i}$”的混淆数发生器 260。混淆数可以是随机数，例如用随机数发生器生成的随机数。混淆数发生器 260 可以生成针对一元多项式的多个系数的多个混淆数。发生器 260 可以被限制为生成单个数字（比如说每个参数集生成一个混淆数或者对于参数集中的至少两个参数集生成一个混淆数），但是发生器 260 还可以被配置成生成非零混淆多项式，其将被加入到相应于当前参数集的一元多项式中，以获取混淆的一元多项式。在实施例中，对一元多项式的每个系数，确定混淆数。混淆多项式可以具有 1、或者 2 或者更多个非零系数。

[0140] 本地密钥材料发生器 200 包括网络设备管理器 250，其被配置成接收必须对其生成本地密钥材料的身份号（例如，从网络设备）并且被配置成向相应于身份号的网络设备发送本地密钥材料。替代接收身份号，其还可以被生成为例如随机数、序列号或者一次性（nonce）数。在后一情况下，身份号与本地密钥材料一同发送到网络设备。

[0141] 多项式操纵设备 240 针对根密钥材料元件 210 中的每个参数集，生成一元多项式。

[0142] 对于每个参数集，多项式操纵设备 240 通过将来自管理器 250 的身份号代入每个二元多项式中并且对每个模相应的私有模数进行归约来获取可能地多个一元多项式。所产生的多个归约的单一多项式在系数方面利用自然运算加法相加。此外，一个或者多个混淆数相加。优选地，结果再次在系数方面通过模公共模数进行归约；后者的系数可以在 0 到 N-1 的范围中表示。

[0143] 混淆的一元多项式是相应于身份号的本地密钥材料的一部分。如果需要的话，公共模数、次数和密钥长度也被发送到网络设备。

[0144] 图 2’ 示出来自根密钥材料 180 的、针对网络设备生成的本地根密钥材料 280。本地根密钥材料 280 包括参数集数量 140（此处为 3）、密钥长度 144、公共模数 141、142 和 143 以及分别对应生成的（可能地混淆的）一元多项式 252、262 和 274。可选地，本地根密钥材料 280 可以包括用于除数的 2 的幂和用于生成共享密钥的密钥模数。

[0145] 图 3 是图示出包括多个网络设备的通信网络 300 的示意性框图；示出了第一网络设备 310 和第二网络设备 320。将说明第一网络设备 310。第二网络设备 320 可以是相同

的，或者以相同的原理工作。

[0146] 网络设备 310 包括收发器 330，其将发送器和接收器相组合以用于以电子（例如，数字）形式有线或者无线地向第二网络设备 320 发送消息并且从第二网络设备 320 接收消息。可能地，收发器 330 还被用来从网络机构 200 接收本地密钥材料。在第二网络设备 320 的图中，通过收发器 330，接收另一个网络设备的身份号。

[0147] 网络设备 310 包括本地密钥材料获取器 344。本地密钥材料获取器 344 可以被实施为本地存储器（例如非易失性存储器，诸如闪速存储器）以用于存储本地密钥材料。本地密钥材料获取器 344 还可以被配置成例如经由收发器 330 从发生器 200 获取本地密钥材料。本地密钥材料获取器 344 被配置成向多项式操纵设备提供所需的参数。

[0148] 网络设备 310 包括多项式操纵设备 342。多项式操纵设备 342 在两个阶段中执行。

[0149] 在代入阶段中，第二网络设备的身份号被代入（530）本地密钥材料中的每个一元多项式中。代入结果的结果被通过模相应于所述一元多项式的公共模数来进行归约。在后续的相加阶段，归约模公共模数的结果被加到一起，并且归约（540）模密钥模数。注意，对于 N 和私有模数的一些组合，在结果通过模密钥模数进行归约之前，需要除以 2 的幂。

[0150] 网络设备 310 包括密钥导出设备 346，其用于从归约模密钥模数的结果中导出共享密钥。例如，密钥导出设备 346 可以移除一个或者多个最低有效比特。密钥导出设备 346 还可以应用密钥导出函数。还可能的是，使用第二次归约的结果，而不进行进一步处理。

[0151] 网络设备 310 包括可选的密钥均衡器 348。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（基于第一网络设备的身份号）导出的密钥。如果这被认为是不合期望的，则可以遵循密钥均衡协议。

[0152] 网络设备 310 包括密码学元件 350，其被配置成将共享密钥用于密码学应用。例如，密码学元件 350 可以在向第二网络设备发送第一网络设备的消息（比如状态消息）前采用共享密钥对其进行加密或者认证。例如，密码学元件 350 可以解密或者验证从第二网络设备中接收的消息的确实性。

[0153] 典型地，用于配置用于密钥共享的网络设备 200 的系统和被配置成确定共享密钥 310 的第一网络设备各自都包括微处理器（未示出），其执行存储在对应设备处的适当软件，例如，该软件可能已经被下载并且存储在相应的存储器（例如，RAM （未示出））中。

[0154] 对于 a=1，尤其是其与 m 的较高值（比如高于 1、2 或者更高、4 或者更高）相组合的情况，获取到一个有趣的实施例。所要求的多项式操纵减少为单次乘法和归约，从而给出尤其简单的实施方式。然而，即使对于这个简单的情况，恢复原始二元多项式也不容易，并且随着 m 的值越高而变得越复杂。虽然甚至对于 a=1 而言，还没有已知的可行的攻击，但是对于未来的分析，线性结构可能是一个起始点，所以出于这个原因，可能希望限制成 a>1。

[0155] 图 4 是图示出生成本地密钥材料的方法 400 的示意性流程图。方法 400 可以由可信的第三方所使用。在步骤 410 中，获取所要求的参数。特别地，获取多个参数集（至少两个）。每个参数集含有公共模数和至少一个私有模数和至少一个二元多项式。在步骤 420 中，例如通过电信网络获取网络设备的身份号。身份号可以在电子消息中被接收。

[0156] 对于每个参数集，重复一次步骤 430。将所获取的身份号代入二元多项式中，并且归约模私有模数。可以存在多个（比如 2 个）二元多项式。在该情况下，对每个二元多项式进行代入，并且将结果以整数运算相加。在步骤 440 中，例如通过加入混淆多项式来将结果

混淆。在简单的实施方式中，混淆可以仅仅是单个系数。步骤 440 是可选的。以这种方式，或者如本文所描述的，一元多项式和公共模数组合被获取，其将形成本地密钥材料的一部分。在步骤 450 中，判定是否剩有参数集，并且如果有，则对于下一个参数集，重复步骤 430 和 440。在步骤 450 中，包括混淆的一元多项式的本地密钥材料被存储在网络设备处。

[0157] 图 5 是图示出生成共享密钥的方法 500 的示意性流程图。方法 500 可以由网络设备来执行。

[0158] 在步骤 510 中，例如通过接收电子消息来获取另一个网络设备的外部身份号。在步骤 520 中，向所述另一个网络设备发送本地身份号。在步骤 510 和 520 之后，本地网络设备和外部网络设备具有彼此的身份号。通过使用它们的本地密钥材料，它们继续进行导出共同的共享密钥。

[0159] 本地网络设备对于其本地密钥材料中的一元多项式重复代入步骤 530。在步骤 530 中，将外部身份号代入以相应的公共模数为模的混淆一元多项式中。在步骤 535 中，判定是否剩有一元多项式，并且如果有，则为本地密钥材料中的下一个一元多项式重复步骤 530。在步骤 540 中，将归约模公共模数的结果加到一起，并且归约模密钥模数。

[0160] 步骤 550 的结果是获取共享密钥的开始。在步骤 550 中，导出共享密钥（比如通过应用密钥导出算法）。在步骤 560 中，向所述另一个网络设备发送密钥确认消息，并且在步骤 570 中，确定密钥是否被确认。如果在步骤 570 中密钥没有被确认，那么方法继续进行到步骤 550 中，导出新的密钥。例如，步骤 550 可以每当密钥未被确认时移除一个附加的最低有效比特。如果密钥被确认，则它可以被用在可选的密码学应用中，或者被本地地存储以供之后使用。

[0161] 步骤 550、560 和 570 一起形成了密钥均衡协议。例如，在步骤 560 中，一次性数和根据在步骤 550 中导出的共享密钥的一次性数的加密可以被发送到第二设备。在步骤 560 中，从第二设备接收消息。所接收的消息可以简单地说明所接收的密钥确认消息示出密钥不相等。所接收的消息还可以含有密钥确认消息。在后一情况下，第一网络设备验证密钥确认消息并且证实密钥是否是相等的。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。

[0162] 图 6 以示意性的形式示出了在两个网络设备（设备 A 和 B）正在生成共享密钥时这两个设备之间的可能的消息序列。时间向下运行。在步骤 610 中，网络设备 A 向设备 B 发送其身份号。在步骤 620 中，设备 B 发送其身份号和其基于身份号 A 和其本地密钥材料导出的共享密钥（K1）的密钥确认消息。在步骤 630 中，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）以获取密钥 K2。在步骤 630 中，设备 A 发送新的密钥确认消息。A 和 B 以这种方式交换密钥确认消息 640，直到它们在步骤 650 中得到相同的密钥为止。在步骤 650 中，设备 A 向设备 B 发送密钥确认消息。设备 B 能够验证它们已经得到了相同的密钥。在步骤 660 中，它发送对其的确认，这可以是认证消息或者密钥确认消息等等。在步骤 670 中，设备 A 发送消息 M1，其是使用现在相等的共享密钥加密（比如使用 AES）和 / 或认证（比如使用 HMAC）的。

[0163] 应意识到，本发明也扩展至适配于将本发明付诸实践的计算机程序，特别是在载体上或中的计算机程序。程序可以是如下形式：源代码、目标代码、源代码和目标代码之间的代码（诸如部分编译的形式）；或者可以是适合于在按照本发明的方法的实施中使用的任

何其他形式。与计算机程序产品有关的实施例包括相应于所阐述的方法中的至少一个方法的每个处理步骤的计算机可执行指令。这些指令可以被细分为子例程和/或被存储在可以静态或者动态链接的一个或者多个文件中。与计算机程序产品有关的另一个实施例包括相应于所阐述的系统和/或产品中的至少一个的每个模块的计算机可执行指令。

[0164] 应该注意的是，上文提到的实施例说明而非限制本发明，并且本领域技术人员将能够设计许多可替换的实施例。

[0165] 在权利要求书中，置于括号之间的任何附图标记不应被解读为限制权利要求。动词“包括”和其词形变化的使用不排除除了在权利要求中记载的那些元件或者步骤之外的元件或者步骤的存在。在元件之前的冠词“一”或者“一个”不排除多个这样的元件的存在。本发明可以凭借包括数个不同元件的硬件来实施，并且可以凭借适当编程的计算机来实施。在列举了数种模块的设备权利要求中，这些模块中的数个模块可以由同一项硬件来体现。某些措施被记载在相互不同的从属权利要求中的单纯事实不指示这些措施的组合不能被有利地使用。

图 1-3 的附图标记列表:	
100	根密钥材料获取器
110	公共模数管理器
112	多项式次数元件
114	密钥长度元件
116	多项式数量元件
122	私有模数管理器
124	对称二元多项式管理器
130,140	二元多项式
180	根密钥材料
200	本地密钥材料发生器
210	根密钥材料元件
240	多项式操纵设备
250	网络设备管理器
252,262,272	一元多项式
260	混淆数发生器
300	通信网络
310	第一网络设备
320	第二网络设备
330	收发机
342	多项式操纵设备
344	本地密钥材料获取器
346	密钥导出设备
348	密钥均衡器
350	密码学元件

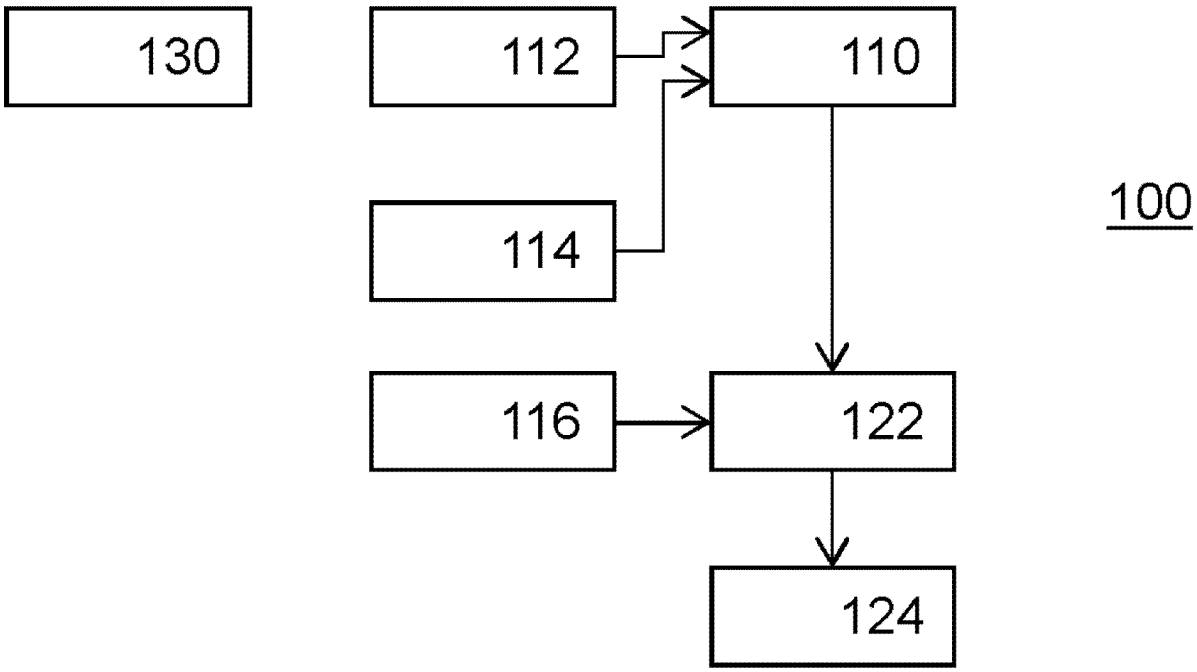


图 1

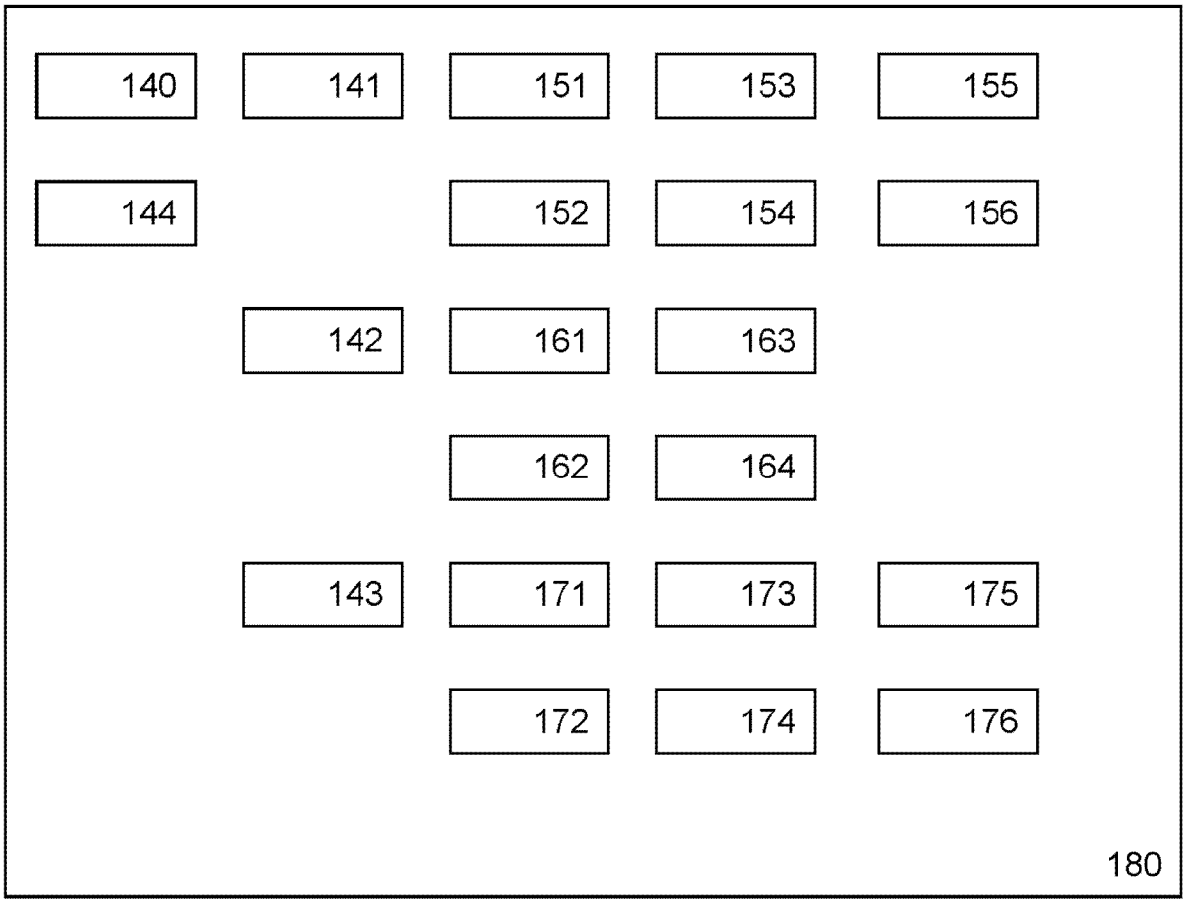

140
141
151
153
155
144
152
154
156
142
161
163
162
164
143
171
173
175
172
174
176
180

图 1'

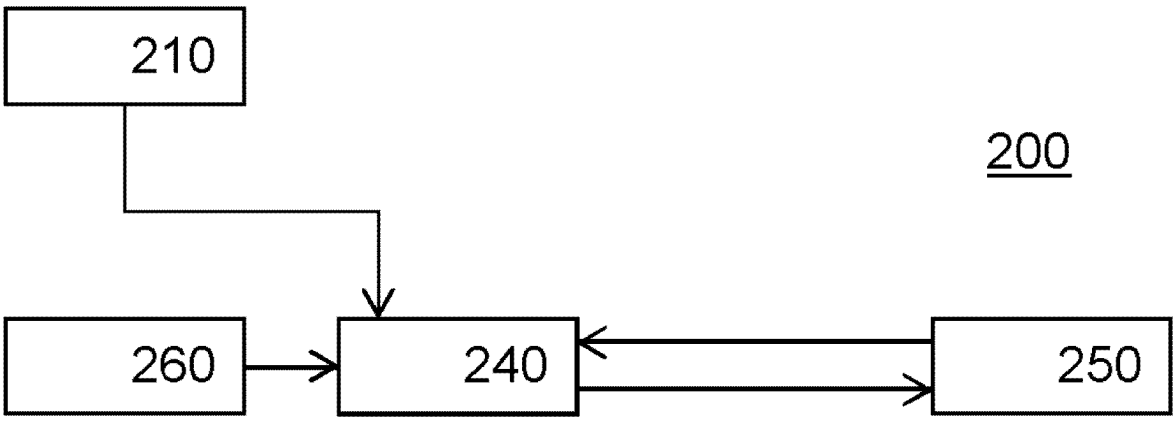

210
200
260
240
250

图 2

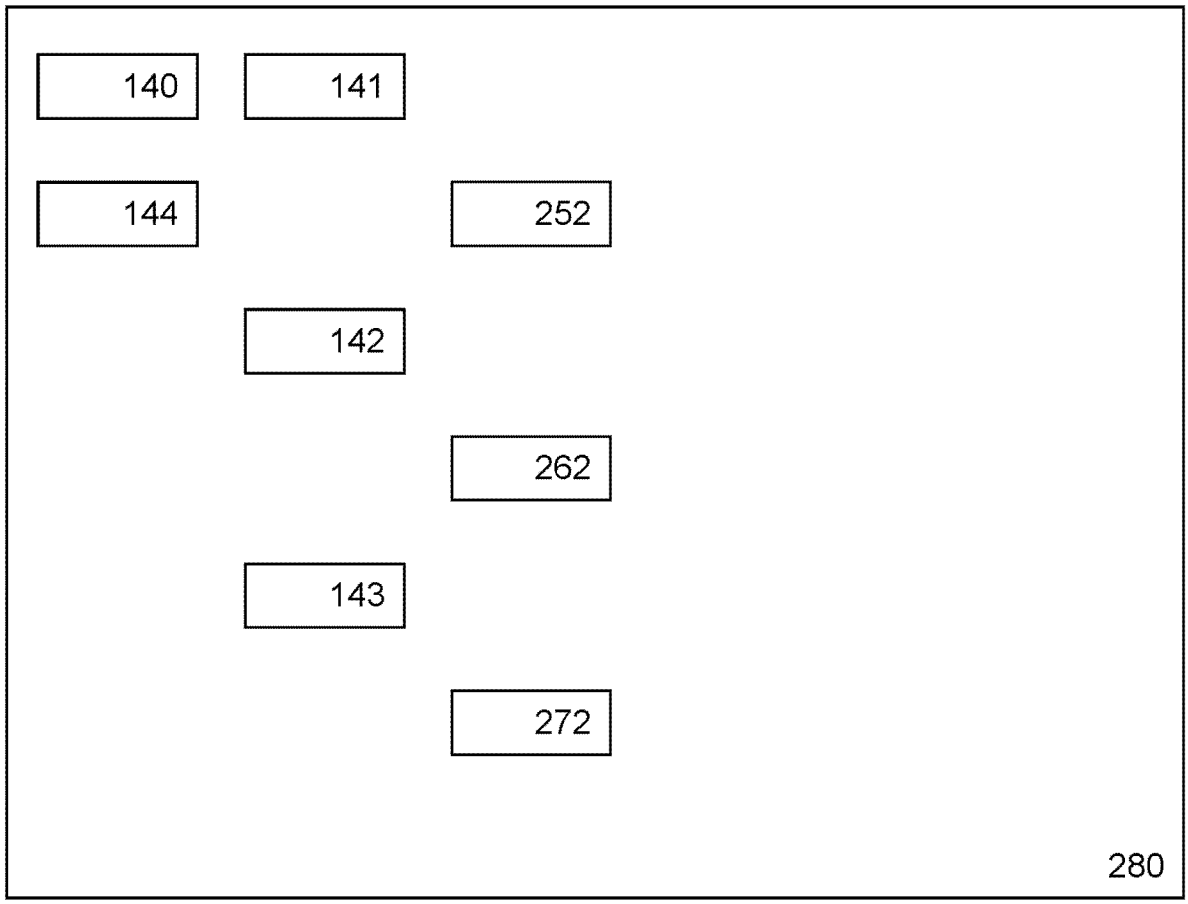


图 2'

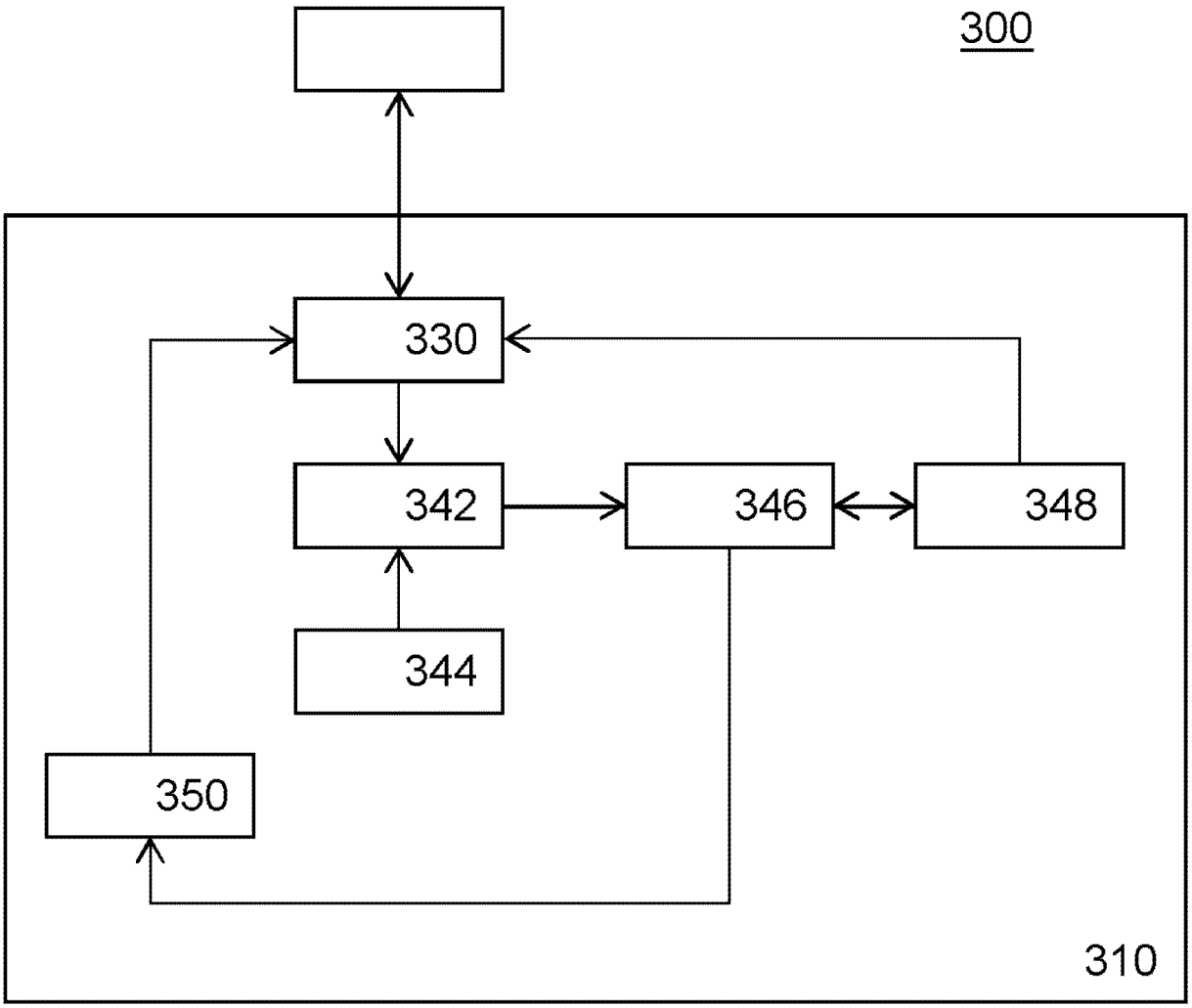


图 3

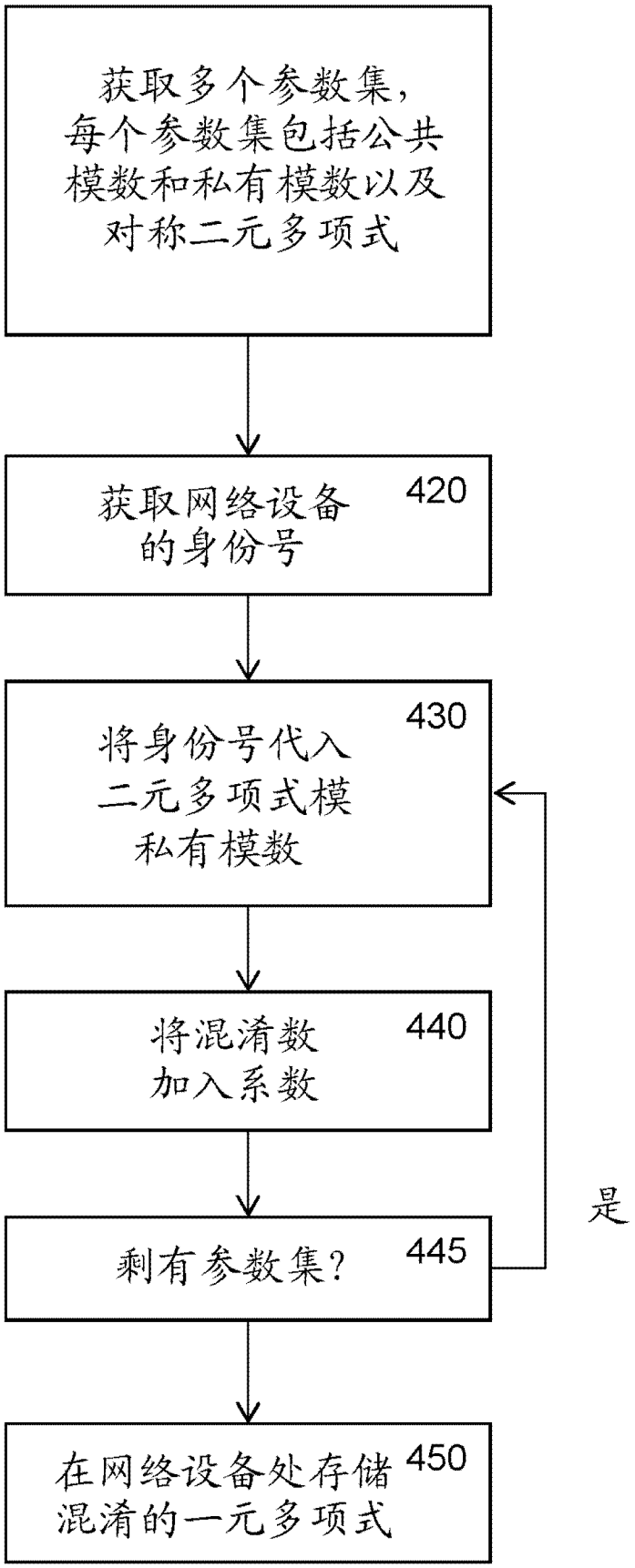

400
获取多个参数集，每个参数集包括公共模数和私有模数以及对称二元多项式
获取网络设备的身份号
420
将身份号代入二元多项式模私有模数
430
将混淆数加入系数
440
剩有参数集？
445
是
在网络设备处存储混淆的一元多项式
450

图 4

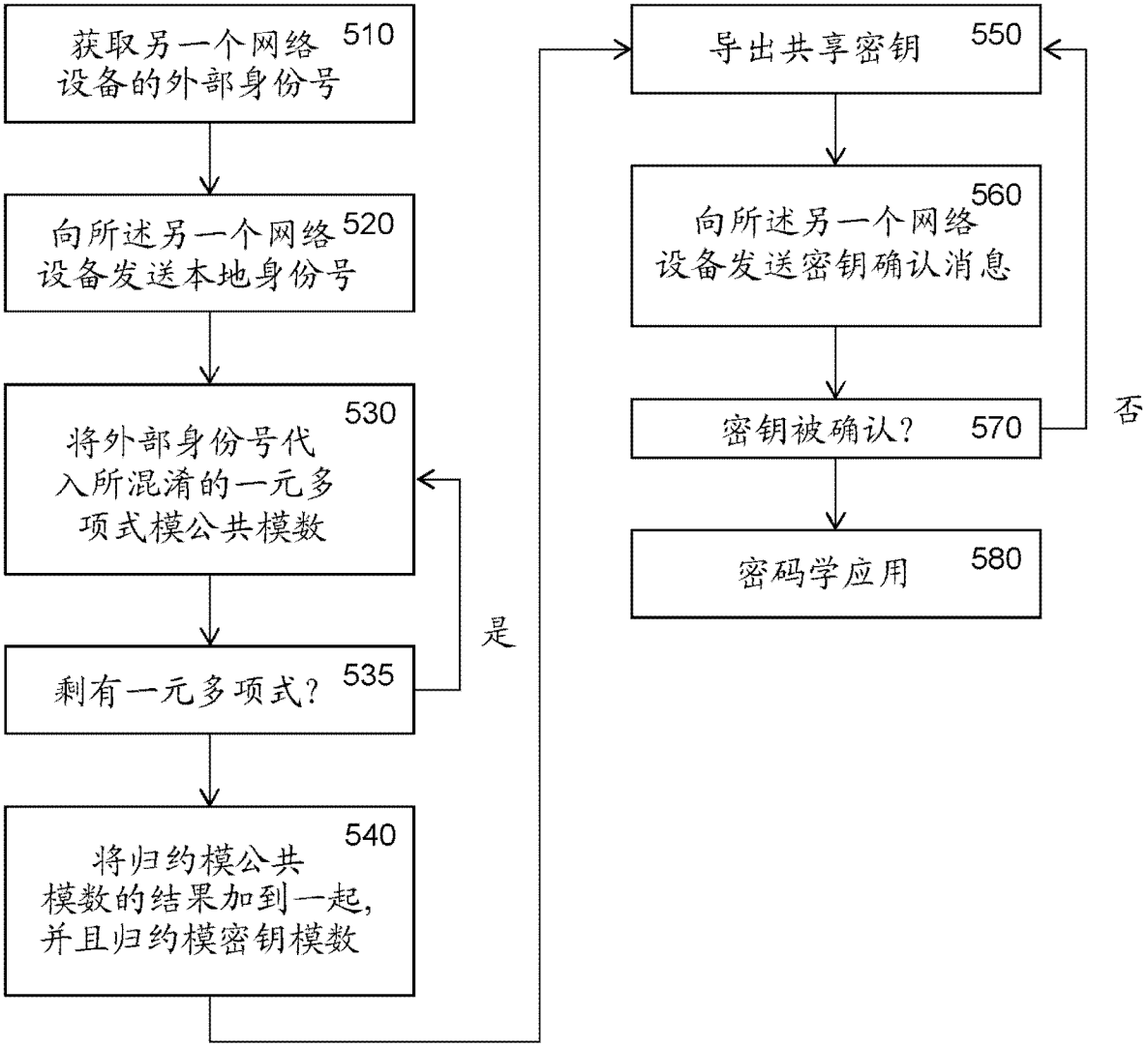

获取另一个网络设备的外部身份号
510
向所述另一个网络设备发送本地身份号
520
将外部身份号代入所混淆的一元多项式模公共模数
530
剩有一元多项式?
535
是
将归约模公共模数的结果加到一起,并且归约模密钥模数
540
导出共享密钥
550
向所述另一个网络设备发送密钥确认消息
560
密钥被确认?
570
否
密码学应用
580

图 5

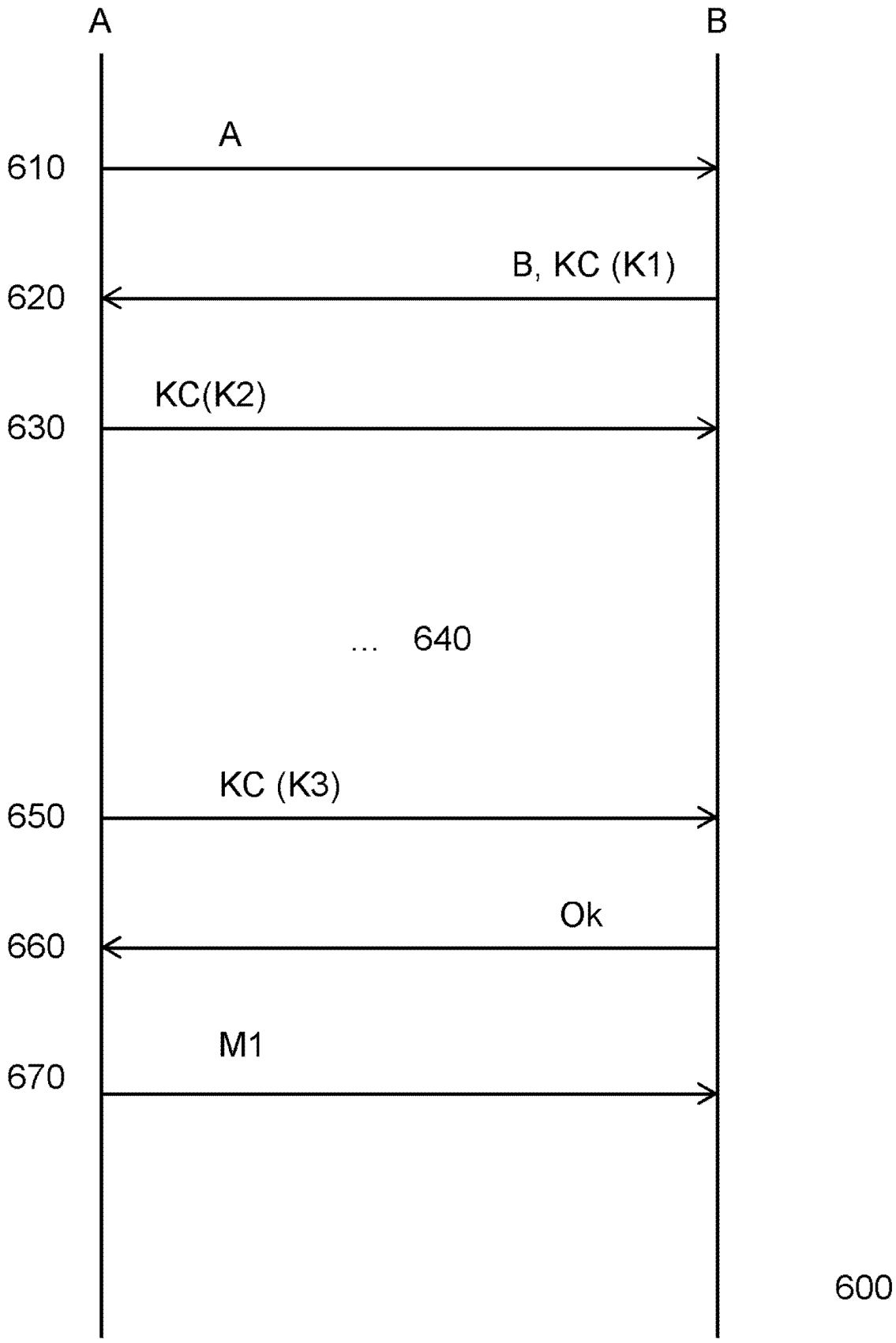


图 6