(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 1773905 B
(45)授权公告日 2010.08.18

(21)申请号 200410090903.X

(22)申请日 2004.11.10

(73)专利权人 日电(中国)有限公司
地址 100738 北京市东城区东长安街1号东方广场东方经贸城东三办公楼1201室

(72)发明人 曾珂 藤田友之

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 王怡

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

(56)对比文件
CN 1258051 A,2000.06.28, 说明书第3页第3段及附图1.
EP 0963635 B1,2003.07.30, 全文.
Lidong Chen.Access with Pseudonyms.Lecture Notes In Computer Science1029.1995,1029232-243.
Brent R.Waters, Edward W.Felten, Amit Sahai.Receiver anonymity via incomparable public Keys.Conference on Computer and Communications Security.2003,112-121.

审查员 谢幸初

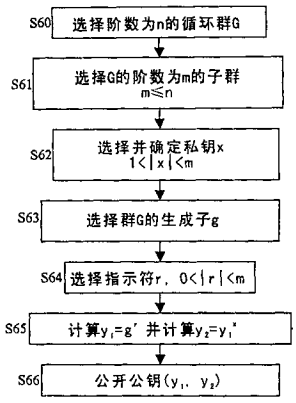
权利要求书 3 页 说明书 10 页 附图 4 页

(54)发明名称

在安全通信系统中生成匿名公钥的方法、设备和系统

(57)摘要

本发明公开了一种产生匿名公钥的方法、设备和系统,用于根据一个私钥,利用一个群的相同生成子来产生多个公钥。还公开了一种公钥加密系统来产生用于安全通信的多个匿名公钥,所有匿名公钥都与同一当事人相关。这些匿名公钥是根据单个私钥,利用相同生成子产生的。利用本发明,可以减少计算量,节省存储器并可提高安全级别。



CN 1773905 B

1. 一种产生公钥以加密要被发送的消息的方法，包括：

选择具有预定阶数的群 G，所述群 G 的阶数是正整数 n；

选择所述阶数内的一个整数 x 作为私钥，其中 x 满足 $1 < |x| < n$；

选择群 G 的元素 g 作为生成子；

选择所述阶数内的整数 r 作为指示符，其中 r 满足 $0 < |r| < n$；

计算 $y_1 = g^r$ 和 $y_2 = y_1^x$ 来产生公钥 (y_1, y_2)；以及

在通信会话之前或在其开始时公开所述公钥 (y_1, y_2)，其中通过选择新的指示符，使用所述私钥 x 和所述生成子 g 产生新的公钥，从而产生多个公钥以用于多个通信会话。

2. 如权利要求 1 所述的方法，还包括：

选择所述群 G 的一个子群，其阶数 m 等于或小于群 G 的阶数 n，基于所述子群来产生公钥；

其中，所述私钥 x 满足 $1 < |x| < m$；并且

其中，所述指示符 r 满足 $0 < |r| < m$。

3. 如权利要求 1 所述的方法，还包括：

基于 y_2 计算一系列公钥。

4. 如权利要求 1 所述的方法，还包括：

存储所述生成子 g 的幂；以及

基于所述所存储的所述生成子 g 的幂，计算新公钥。

5. 如权利要求 4 所述的方法，还包括：

使用所述生成子 g 的所述所存储的幂来计算新公钥为所述所存储的幂的乘积。

6. 一种用于产生多个公钥的计算设备，包括：

群选择器，用于选择具有预定阶数的群 G，所述群 G 的阶数是正整数 n；

寄存器，用于存储所产生或选择的信息；

整数选择器，用于选择所述阶数内的一个整数作为私钥 x，并选择所述阶数内的一个整数 r 作为指示符；

生成子选择器，用于从所述群 G 中选择一个元素 g 作为生成子；

群运算器，用于执行所述群 G 上的群运算；

产生模块，用于通过计算 $y_1 = g^r$ 和 $y_2 = y_1^x$ 来产生公钥 (y_1, y_2)，并且当选择一个新指示符时，产生一个新的公钥，从而利用所述私钥 x 和所述生成子 g 产生所述多个公钥；以及

控制单元，用于控制所述群选择器、寄存器、整数选择器、生成子选择器、群运算器和产生模块的操作。

7. 如权利要求 6 所述的设备，还包括：

子群选择器，用于选择所述群 G 的一个子群，其阶数是 m，并且 m 小于或等于所述群 G 的阶数 n，

其中，基于所述子群来产生公钥，并且所述私钥 x 和所述指示符 r 分别满足 $1 < |x| < m$ 和 $0 < |r| < m$。

8. 如权利要求 7 所述的设备，其中所述寄存器还存储所述生成子 g 的幂，所述幂被所述产生模块用来产生新的公钥。

9. 如权利要求 8 所述的设备，其中，基于多个所存储的幂，计算一个新的公钥为所存储

的幂的乘积。

10. 如权利要求 6 所述的设备，其中所述控制单元、群选择器、寄存器、整数选择器、生成子选择器、群运算器和产生模块中的任何一个都实现为软件、硬件或软件与硬件的结合。

11. 一种通信方法，包括：

选择具有预定阶数的群 G，所述群 G 的阶数是正整数 n；

选择所述阶数内的一个整数 x 作为私钥，其中 x 满足 $1 < |x| < n$；

选择群 G 的元素 g 作为生成子；

选择所述阶数内的整数 r 作为指示符，其中 r 满足 $0 < |r| < n$；

计算 $y_1 = g^r$ 和 $y_2 = y_1^x$ 来产生公钥 (y_1, y_2)；

公开所述公钥 (y_1, y_2)；

利用所述公钥 (y_1, y_2) 来加密一个消息 M，得到一个加密消息 C；

通过通信信道发送所述加密消息 C；

在所述通信信道上接收所述加密消息 C；以及

利用所述私钥 x 来解密所述加密消息 C，以恢复出所述消息 M，其中

通过选择多个不同的指示符，使用所述私钥 x 和所述生成子 g 来产生多个不同的公钥以用于多个不同的通信会话。

12. 如权利要求 11 所述的方法，还包括：

选择所述群 G 的一个子群，其阶数 m 等于或小于群 G 的阶数 n，基于所述子群来产生公钥；

其中，所述私钥 x 满足 $1 < |x| < m$；并且

其中，所述指示符 r 满足 $0 < |r| < m$。

13. 如权利要求 12 所述的方法，其中通过下述步骤来从所述消息 M 计算所述加密消息 C：

选择一个整数 k 作为指定符，满足 $1 < |k| < m$；并且

通过计算 $C = (C_1, C_2)$ 来计算所述加密消息 C，其中 $C_1 = y_1^k$，$C_2 = M \odot y_2^k$，$\odot$ 是群 G 上的可逆运算，并且其中当接收到所述加密消息 C 时，从该消息获取 C1 以用于产生新的公钥。

14. 如权利要求 13 所述的方法，其中当接收到多个加密消息时，基于所接收到的加密消息的若干部分的乘积，产生一系列新的公钥。

15. 一种通信系统，包括：

一个或多个编码设备；

具有一个私钥 x 的一个解码设备，其中，所述私钥 x 被选择为具有预定阶数的群 G 的阶数内的一个整数，所述群 G 的阶数是正整数 n，x 满足 $1 < |x| < n$，且所述群 G 的元素 g 被选择作为生成子；以及

一个或多个通信信道，所述编码设备可通过所述通信信道与所述解码设备通信；

其中，

当在所述通信信道之一上开始一个新的通信会话时，所述解码设备根据所述私钥 x，利用所述群 G 的相同生成子 g，通过选择所述群 G 的阶数内的新的整数 r 作为指示符，其中 r 满足 $0 < |r| < n$，计算 $y_1 = g^r$ 和 $y_2 = y_1^x$，来产生一个新的公钥 (y_1, y_2)。

16. 如权利要求 15 所述的系统，其中所述解码设备存储所述生成子 g 的幂，用于计算新

的公钥。

17. 如权利要求 16 所述的系统，其中当在所述解码设备中接收到加密的消息时，该消息被用来产生新的公钥。

18. 一种产生公钥以加密要被发送的消息的装置，包括：

用于选择具有预定阶数的群 G 的装置，所述群 G 的阶数是正整数 n；

用于选择所述阶数内的一个整数 x 作为私钥的装置，其中 x 满足 $1 < |x| < n$；

用于选择群 G 的元素 g 作为生成子的装置；

用于选择所述阶数内的整数 r 作为指示符的装置，其中 r 满足 $0 < |r| < n$；

用于计算 $y_1 = g^r$ 和 $y_2 = y_1^x$ 来产生公钥 (y_1, y_2) 的装置；以及

用于在通信会话之前或在其开始时公开所述公钥 (y_1, y_2) 的装置，

其中，通过选择新的指示符，所述用于产生公钥的装置使用所述私钥 x 和所述生成子 g 产生新的公钥，从而产生多个公钥以用于多个通信会话。

19. 一种通信装置，包括：

用于选择具有预定阶数的群 G 的装置，所述群 G 的阶数是正整数 n；

用于选择所述阶数内的一个整数 x 作为私钥的装置，其中 x 满足 $1 < |x| < n$；

用于选择群 G 的元素 g 作为生成子的装置；

用于选择所述阶数内的整数 r 作为指示符的装置，其中 r 满足 $0 < |r| < n$；

用于计算 $y_1 = g^r$ 和 $y_2 = y_1^x$ 来产生公钥 (y_1, y_2) 的装置；

用于公开所述公钥 (y_1, y_2) 的装置；

用于利用所述公钥 (y_1, y_2) 来加密一个消息 M，得到一个加密消息 C 的装置；

用于通过通信信道发送所述加密消息 C 的装置；

用于在所述通信信道上接收所述加密消息 C 的装置；以及

用于利用所述私钥 x 来解密所述加密消息 C，以恢复出所述消息 M 的装置，

其中，通过选择多个不同的指示符，所述用于产生公钥的装置使用所述私钥 x 和所述生成子 g 来产生多个不同的公钥以用于多个不同的通信会话。

在安全通信系统中生成匿名公钥的方法、设备和系统

技术领域

[0001] 本发明涉及计算机通信网络安全，更具体地说涉及公钥加密通信系统和方法。

背景技术

[0002] 随着计算机通信网络的发展，例如 IP 网络、电信网络、移动自组织网络和私有局域网络等，已在这些计算机通信网络上开发并部署了许多应用。这些应用包括医疗保健系统、电子处方系统、电子邮件系统、电子购物系统、电子拍卖系统、多媒体系统、收费电视系统、基于位置的服务系统以及普适计算系统等等。然而，通过这些系统传输的信息（更一般地说是数据）容易受到黑客攻击、监听、窃听、篡改和操纵等等。虽然对安全性和隐私的关注程度可能因应用而有所不同，并明显地因人而异，但是，发送者将数字化信息安全地传递给接收者，并且第三方和接收者都不能危及信息的安全性，这是一个基本的需求。另外，需要将发送者以及接收者的隐私保护到一个令人满意的程度。

[0003] 保护信息的安全性的一个示例是安全电子邮件系统。在此情形下，只有发送者和接收者可以解读该电子邮件。另一个示例是安全电子支付系统，其中只有帐户的所有者才能花费该帐户中的资金。

[0004] 许多情形下的信息隐私问题需要获得与信息安全问题相当甚至更高的关注。考虑前面提到的安全电子邮件和安全电子支付系统，其中电子邮件和电子支付系统的使用者希望自己之外的任何人都不知道通信的存在。为了保护电子邮件中发送者的隐私，在一些情形下可能必须使得甚至连接收者也不能获知发送者是谁。对于电子支付交易，有时可能希望收款人不能识别出付款人。对于信息隐私还存在许多其他示例。在利用基于位置的服务时，携带移动设备的所有者的位置在大多数情形下都处于该所有者的完全控制之下。在电子购物中，付款人可能希望防止在线商家对其购买历史进行关联，然后推测出其个人兴趣。在电子拍卖中，出价者可能希望防止竞争者分析其出价策略，并然后使用这一知识来击败他。其他示例包括匿名成员资格管理和用于电子投票的匿名投票者等等。

[0005] 一般地，加密通信系统始于在远程位置之间传输消息。这种系统包括第一位置处的至少一个编码设备，以及第二位置处的至少一个解码设备，该编码设备和解码设备都耦合到计算机通信网络。对于数字化系统，消息可以定义为数字化消息，即某个字母表的符号序列。实际中，一般将字母表选择为由符号 0 和 1 组成的二进制字母表。在典型的通信会话中，每个用户的终端通常都同时配备有编码器和解码器，以使得用户可以向另一个用户发送加密信息并从其接收加密信息。

[0006] 传统上，可很容易地获得多种公钥加密编码和解码技术，以提供一定程度上的安全性和隐私性。例如授权给 Rivest 等人的美国专利 No.4,405,829(RSA) 以及 ElGamal(Tahir ElGamal.A public-key cryptosystemand a signature scheme based on discrete logarithms.Advances in Cryptology Proceedingsof CRYPTO 84,pages 10-18,1985) 是本领域内公知的技术。Rivest 专利和 ElGamal 的教导通过引用而被包含。

[0007] 在公钥加密系统中，每个用户（例如用户 A）在一个公共文件中放置加密算子或公

钥 E_A。用户 A 将对应的解密算子或私钥 D_A 保密，其对于任何消息 M 都满足下面的公式

[0008] $D_A(E_A(M)) = M$。

[0009] 为使得该公钥系统可实际运行，E_A 和 D_A 都必须是实际可计算的。然而，用户 A 在公开 E_A 时不能危及 D_A。也就是说，对于任何对手来说，只给出加密密钥 E_A 和一些可能的明文和密文对，寻找一个有效的方式来计算 D_A 在计算上是不可行的。在公钥系统中，慎重地选择密钥确保了只有用户 A 才能实际计算出 D_A。

[0010] 另一个用户（例如用户 B）希望向用户 A 发送消息 M 时，他在所述公共文件中寻找 E_A，然后将加密的消息 $E_A(M)$ 发送给用户 A。接收后，用户 A 通过下面的公式来解密该消息：

[0011] $D_A(E_A(M)) = M$。

[0012] 由于实际上不能从 E_A 导出 D_A，因此只有用户 A 可以解密发送给他的消息 $E_A(M)$。类似地，如果用户 A 希望向用户 B 发送消息作为响应，用户 A 使用用户 B 的加密密钥 E_B 来加密响应消息，E_B 也可在所述公共文件中获得。这一安全通信过程意味着每个希望接收私密通信的用户都必须将他的加密密钥 E 放置在公共文件中。或者换句话说，为了安全地与他人通信，利用传统的公钥加密系统例如 RSA 和 El Gamal，用户 A 需要向外部世界公开他/她的公钥。然而，在大多数情形下，用户 A 只拥有一对公/私钥对，即一个公钥和其对应的唯一的私钥。公钥系统这一典型的使用方式存在一个不希望出现的后果，即使得用户 A 的公钥完全成为了他/她的标识。这意味着即使关心隐私的用户得到了这类公钥加密系统以及其他设计得很好的隐私保护措施的保护，对手仍能够基于该唯一公钥的使用模式，通过收集并观测该用户公开的信息，从而关联出受保护的用户的活动。

[0013] 在信息时代，隐私被广泛地视为信息交换的一个突出关注点。隐私调查持续显示出 80-90％的人群关注隐私，并且 25％的人群愿意支付相当的金钱或容忍一些不方便来获得隐私性。这种隐私保护的重要性不仅显示出现有公钥加密系统的缺点，还突出了新的改进的匿名公钥方法的重要性和紧迫性。

[0014] 在传统的公钥加密系统（例如 RSA 和 El Gamal 所公开的系统）中，如果用户 A 担心他/她的单个公钥可能会危害他/她的隐私，则可以消除单个公钥的可标识特性。解决办法仅仅是要求所述个体例如用户 A 拥有若干不同的公钥，并在例如拍卖中向不同的通信对方公开这些公钥中的不同公钥。

[0015] 在拥有许多公钥对之外，Waters 等人已提出了一种方法，其利用 ElGamal 加密系统来实现了一种“不可比公钥方案”，借此用户可以同时拥有若干公钥，而所有这些公钥都对应于单个私钥。参见 B.R.Waters，E.W.Felten，A.Sahai，Receiver Anonymity via Incomparable Public keys，CCS’03，Washington，DC，USA，pp.112 ～ 121。Waters 等人的教导通过引用也被包含。

[0016] 通过利用多个公钥对，传统的公钥加密系统可以在一定程度上减弱隐私问题。然而，所述个体仍远不能满足。事实上，这一措施有许多缺点。其一，每个不同的公钥都具有对应的不同的私钥，这就意味着随着公钥的数量增加，对于个人来说公私钥对的管理成本也在增加。其二，每个不同的公钥具有对应不同的私钥意味着随着私钥数量的增加，私钥被公开或丢失的安全性风险也在增加。其三，考虑一个人拥有 100 个公钥对，在传统公钥加密系统来说这对一个人是相当多了。假设此人希望在并行或串行的通信中与 200 个通信对方通信。结果，这些通信对方中至少有两人会接触到该关心隐私的个人的同一公钥。最后，加

密消息的接收者可能必须尝试所有的私钥来解密该消息，这是非常耗时又低效的。

[0017] Waters 等人的方案看起来能够消除若干公钥对的管理成本以及随之而来的安全性风险。然而，他们的不可比公钥方案通过利用不同的生成子 (generator) 来构建 ElGamal 加密系统的公钥，从而生成新的公钥，这使得计算优化变得很困难。例如，(g, g^a) 和 (h, h^a) 是通过 Waters 等人的不可比公钥方案生成的不同公钥，其中 g 和 h 是不同的生成子。传统上，ElGamal 加密系统只利用了一个生成子，因此能够受益于在线计算生成子的幂并只维护一张生成子的幂表。而 Waters 等人的方案需要要么维护若干张生成子的幂表，要么进行在线计算，从计算优化和成本管理来说二者都不太可取。

发明内容

[0018] 本发明公开了一种公钥加密系统，用于生成用于安全通信的多个匿名公钥，所有这些公钥都与同一当事人相关。而且，这些匿名公钥是使用相同的生成子而从单个私钥产生的。

[0019] 根据本发明的一个方面，提供了一种产生公钥以加密要被发送的消息的方法，包括：选择一个私钥；使用所述私钥和一个生成子来产生公钥，所述私钥和所述生成子来自一个预定的群；以及在通信会话之前或在其开始时公开所述公钥，其中使用所述私钥和所述生成子来产生多个公钥以用于多个通信会话。

[0020] 更具体地说，本发明公开了若干方法和设备，用于基于同一个生成子 g，从私钥 x 计算产生多个公钥，这些公钥具有 $(y_1 = g^r, y_2 = y_1^x)$ 的形式，其中在不同的通信会话中或与不同的通信对方通信时，当选择一个不同的 r 时，就产生一个新的公钥。

[0021] 更具体地说，本发明基于数学中公知的群论的应用和实现。假设 G 是有限循环群。选择群 G 的元素 x 作为解密密钥（私钥）D。假设 g 是群 G 的生成子。这样，加密密钥（公钥）E 由一对 G 的元素 y_1 和 y_2，构成，计算如下：

[0022] $y_1 = g^r$

[0023] $y_2 = (y_1)^x$，

[0024] 其中 r 是整数（以下称为“指示符”）。如果 y_1 和 y_2 原来在群 G 的范围之外，则它们必须被映射到群 G 内。映射方法根据所选择的群而各有不同。

[0025] 而且，当选择一个不同的指示符 r 时，产生了一个新的公钥。

[0026] 加密设备可如下加密明文消息 M：

[0027] $C_1 = y_1^k$

[0028] $C_2 = M \odot y_2^k$

[0029] $C = (C_1, C_2)$

[0030] 其中 k 是整数（以下称为“指定符”），⊙是群 G 上的可逆运算，C_1 和 C_2 是群 G 的元素。

[0031] 当从发送者接收到密文 C 时，接收者处的解密设备可如下将 C 转换成消息字 M′（即重建明文）

[0032] $t = C_1^{-x}$

[0033] $M' = t \odot C_2$

[0034] 其中 M′ 是群 G 的元素，⊙是群 G 上的可逆运算。

[0035] 如果一个要加密的消息位于群 G 的范围之外，在加密前它必须被转换成若干个群元素。在随后的解密之后，所恢复出的群元素可被转换回到初始的消息。对于不同的群或不同的实现来说转换方法各有不同。

[0036] 如果 C_1 或 C_2 一开始就在群 G 的范围之外，它们必须被映射到群 G 内。对于不同的群或不同的实现来说映射方法各有不同，并且对于本领域内的技术人员来说是公知的。

[0037] 通过选择指示符 r，用户可以产生对应于单个私钥 x 的许多公钥。

[0038] 相应地，用户只需维护一张表来存储生成子的幂，并可以离线地计算它们，因此避免了在线计算的额外开销。

[0039] 与基于 Waters 等人的方案的安全通信系统相比，本发明公开了一种用于安全通信系统的新型匿名公钥技术。本发明利用了生成子的幂（即指数）来构建匿名公钥，而 El Gamal 加密系统和 Waters 等人的方案直接使用生成子来构建公钥。

[0040] 相比于现有技术，本发明至少具有下述优点：

[0041] 其一，本发明使得关心隐私的人们可以向通信对方公开他 / 她的公钥，以在通信历史很重要的场合建立安全通信。

[0042] 其二，本发明基于了一种新型技术，其中多个公钥对应于单个私钥，因而极大地降低了个人对公钥对的管理成本，并在最大程度上降低了与私钥有关的安全性风险。

[0043] 其三，本发明实现的新型优化技术可以使得以较低的成本来采用所建议的匿名公钥，并将计算密集型的任务转移到离线进行或计算系统的非高峰时间。

[0044] 其四，本发明可以通过实际并有效地将部分计算负担转移到通信对方来减少不可避免的计算开销，而不会向通信对方引入额外的成本。

[0045] 其五，本发明实现的新型优化技术可以有效地减少公钥的存储消耗。

[0046] 其六，通过匿名公钥，本发明自然地确保了私钥的匿名性。与此相对比的是，利用传统的公钥加密技术，私钥不可避免地通过唯一的公钥而被识别，尽管私钥的准确值是保密的。这在一些情形下为本发明获得了一种可能的利用方式，其中用户可以拥有若干私钥，并分别为不同的私钥产生一系列匿名公钥。在这种意义下，所使用的私钥也被匿名化了，也就是说，它们是匿名私钥。

附图说明

[0047] 通过下面的描述，并结合附图来阅读时，可更透彻地理解本发明前述及其他目的、各种特征以及本发明本身，在附图中：

[0048] 图 1 示出了一个具有两个终端的示例性系统，其利用了根据本发明的匿名公钥加密系统，其中所述终端之一可以公开一个不同的公钥来用于与另一个终端的新通信会话；

[0049] 图 2 示出了具有若干终端的示例性系统，其利用了根据本发明的匿名公钥加密系统，其中一个终端在与其他终端的通信中可以使用不同的公钥来用于不同的会话；

[0050] 图 3 示出了参与图 1 和图 2 的通信系统的发送者和接收者之间的示例性通信会话；

[0051] 图 4 示出了基于根据本发明的公私钥对的通信会话中，发送者和接收者的示例性功能模块；

[0052] 图 5 示出了根据本发明，图 4 中的公钥产生设备的示例性功能模块；

[0053] 图 6 示出了根据本发明，产生匿名公钥的示例性流程图；并且

[0054] 图 7 示出了消息的加密与解密的示例性过程。

具体实施方式

[0055] 在此公开了在安全通信系统中产生匿名公钥的方法、设备和系统。在下面的详细描述中，给出了大量具体细节以完整地理解本发明。然而应该认识到，对于本领域内的技术人员来说，在没有这些具体细节中的一些的情况下也可以实施本发明。在其他情形下，没有详细示出一些公知结构和技术，以免不必要地混淆本发明。

[0056] 在整个说明书中，术语“群”(group) 指的是如下定义的数学概念（除非另有说明）：

[0057] 群 (G,◇) 由满足如下三个规律的集合 G 及其上的二元运算◇构成：

[0058] (i) 群运算满足结合律，即对于 G 的任意元素 a、b、c，有 a ◇ (b ◇ c) = (a ◇ b) ◇ c；

[0059] (ii) 集合 G 存在一个基元 e，对于任何 G 的元素 a 都有 a ◇ e = e ◇

[0060] a = a；

[0061] (iii) 对于 G 的任何元素 a，G 中都存在一个元素 a^{-1}（称为 a 的逆元），满足 $a \diamond a^{-1} = a^{-1} \diamond a = e$。

[0062] 例如，整数集 Z 及加法运算构成一个群。基元是 0，一个整数 a 的逆元是 -a。对于更多的信息，可以参考《Handbook of AppliedCryptography》，可在 http://www.cacr.math.uwaterloo.ca/hac/ 在线获得。

[0063] 根据本发明的通信系统可具有若干终端和若干通信信道。图 1 以简化框图示出了本发明的一个实施例。在图 1 中，终端 A 与终端 a 进行了若干次会话的通信。对于终端 A 来说，至少存在一个通信信道来向终端 a 发送信息。所述会话可能使用一个或若干通信信道。终端 a 可能也可能不使用相同的通信信道来向终端 A 发送信息。通过所述通信信道，终端 A 向终端 a 公开不同的公钥 E_a 到 E_z 来用于不同的通信会话，但将它的私钥 x 保密。如果终端 a 需要的话，也可以向终端 A 公开若干不同的公钥，在此意义上终端 a 等同于终端 A。

[0064] 如图 1 所示，通过产生不同的公钥来用于不同的会话，对于终端 a 或任何第三方来说都不可能关联出终端 A 的活动模式。例如，在电子拍卖的场合中，终端 A 的用户将能够防止他人关联并分析其出价模式和策略，这是因为对于每次会话都产生了不同的公钥。

[0065] 图 2 也以简化框图的形式示出了本发明的另一个实施例。在图 2 中，终端 A 与多个终端（从终端 a 到终端 z）通信。终端 A 与其每一个通信对方之间所使用的通信信道可能相同也可能不同。如图 2 的左半部分所示，通过所述通信信道，终端 A 分别向终端 a、终端 b、……、终端 z 公开了不同的公钥 E_a 到 E_z 以及其他信息。在此情形下，我们认为在终端 A 和终端 a 到 z 之间存在一种“一对多”的关系。所述公开可以多种方式完成。例如，可以有其他信息与所述公钥一起公开，或者所述公钥可以包含在电子邮件或证书中。反过来，终端 a 和终端 z 可能也可能不使用相同的通信信道（在所述通信信道上，这些终端中的每一个接收到终端 A 的公钥）来向终端 A 发送信息，这些信息已用所接收的公钥加密。如前所述，终端 A 将自己的私钥 x 保密。类似地，如果终端 a 到终端 z 需要的话，可以向终端 A 分别公开若干不同的公钥，在此意义上终端 a 到终端 z 等同于终端 A。类似地，从图 2 的右半部分

可看出，终端 a 到 z 分别向终端 A 公开各自的公钥 E_a 到 E_z。在此情形下，我们认为在终端 a 到 z 和终端 A 之间存在一种“多对一”的关系。

[0066] 图 3 示出了参与图 1 和图 2 所示的通信系统中的发送者和接收者之间的示例性通信会话。在图 3 中，每一次发送者希望向接收者公开公钥时，发送者都决定（步骤 S31）或者是从它现有的公钥池中选择一个公钥（步骤 S32），或者产生一个新的公钥（步骤 S33）。然后，发送者将公钥发送给接收者（步骤 S34）。需要发送消息时（步骤 S35），接收者查找发送者的公钥（步骤 S36）以加密消息（步骤 S37），然后将加密的消息发送给发送者。最终，发送者解密所接收的加密消息（步骤 S38），并恢复出发送自接收者的原始消息。注意，接收者可能在它要向发送者发送加密消息之前很久就已经从发送者接收到了所述公钥。

[0067] 应指出的是，发送者可以被设计成总是产生不同的公钥（步骤 S33）而不依赖于任何现有的密钥。然而，如本领域内的技术人员可以认识到的那样，使用现有公钥池将可大大减少计算开销，这是因为操纵现有公钥比起从头开始计算来说内在地要少很多计算量。

[0068] 还应该指出的是，图 3 中的发送者和接收者的指定只是出于方便的考虑，因为发送者首先将它的公钥发送给接收者。接收者接收到来自发送者的公钥之后，接收者在向它的“接收者”（所述发送者）发送加密消息时就成了“发送者”。在两个终端之间的典型双向通信会话中，所述角色在整个会话中会频繁颠倒。

[0069] 现在参考图 4，其示出了基于根据本发明的公私钥对的通信会话中，发送者和接收者的示例性功能模块。在此，发送者 41 至少包括处理通信信道的发送单元 43 和接收单元 45、处理密文解密的解码设备 47、以及处理公钥产生的公钥产生设备 49。接收者 42 至少包括发送单元 44、接收单元 46、以及处理将要发送的信息例如明文的加密的编码设备 48。发送者 41 可向接收者 42 公开多个公钥，以使得如果发送者 41 和接收者 42 之间存在多个会话，则每个会话可使用发送者 41 不同的公钥。如果发送者 41 也工作为接收者，则它还可包括一个编码设备 48。类似地，如果接收者 42 工作为发送者，则它还可包括一个解码设备 47 和公钥产生设备 49。

[0070] 图 4 中的编码设备 48 和解码设备 47 都是数据通信和加密领域中公知的。下面的图 5 进一步示出了公钥产生设备 49。参考图 5，控制单元 55 处理产生公钥以及管理公钥的过程。寄存器 54 可用来存储私钥、所产生的公钥、所接收的公钥以及其他控制单元 55 所需的数据。另外，在此所使用的寄存器 54 可以通过可存储信息的任何器件实现，例如片上寄存器、ROM 和 RAM。公钥产生设备 49 可与解码设备 47 共享寄存器 54，以存储所接收的密文以及解密时的中间输出。下面将描述公钥产生设备 49 的其他组件。

[0071] 注意，在图 5 中，“群”运算是由群指数运算器 57 处理的。公钥产生设备 49 也可有其他实施方式，其中的群运算由一个独立的群运算器处理。

[0072] 下面将描述图 4 和图 5 的公钥产生设备 49 根据本发明产生匿名公钥（“APK”）的过程。

[0073] 图 6 示出了产生 APK/ 私钥对的示例性处理流程。首先，群选择器 51 选择一个群 G（步骤 S60）。例如，计算机可具有存储器，其中存储了代表各种符合条件的群的各种数据结构。在控制单元 55 的控制下，群选择器 51 通过选择代表群的数据结构来选择一个群。在实践中，已经存在一些商用函数库，其可以运行在计算机上并提供这种服务。需要实现本发明的应用程序可利用一些具体参数来调用这种库提供的特定函数。然后所调用的函数就

可以返回所需的（多个）群。在一个实施例中，G 是有限循环群，其阶数是 n（n 是正整数）。有限循环群 G 的候选者包括但不局限于：

[0074] 有限域 F_{q1} 上的椭圆曲线上的点构成的群；

[0075] 有限域 F_{q2} 上的乘法群 F_{q2}^*，其中 $q2 = p^{m1}$，m1 是正整数，p 是素数；

[0076] 群 Z_{n1}^*，其中 n1 是合数；以及

[0077] 乘法群 Z_{n2}^*，其中 n2 是素数。

[0078] 在上述四中示例性群中，第一种群可能具有最佳的安全性能，而后三种在本领域中使用得更为普遍。群 G 的“有限循环”特性确保了群指数运算最终都会被映射到群 G 内；然而，映射方法可能会根据群而不同。另外，它还确保了生成子的存在。

[0079] 然后，子群选择器 52 选择 G 阶数为 m 的子群，其中 $m \leq n$（步骤 S61）。如果 m 选择为素数，则将具有优选的安全性能。请注意所述子群可被选择为 G 自身，这也就意味着 $m = n$。在另一个实施例中，假设在群 G 被确定或选择后，可省略子群的选择，这也意味着 G 自身被隐式地选择为所述子群，因为在数学上 G 是它自身的一个子群。也就是说，当 G 本身被选择为所述子群时（使得 $m = n$），则这一选择可在表面上被省略。当然，如果省略子群的选择，则也可省略子群选择器 52（如图 5 所示）。

[0080] 然后，整数选择器 56 选择一个整数作为私钥 x，使得 x 满足 $1 < |x| < m$（步骤 S62）。应理解到，一个终端可具有多个私钥，尽管在此的描述为了简单起见集中于如何从一个私钥生成多个公钥。

[0081] 然后，生成子选择器 53 选择并确定群 G 的一个生成子（步骤 S63）。如果 G 是有限循环群，则它总会有至少一个生成子。应注意，g 和 x 的选择是彼此独立的。也就是说，尽管步骤 S62 在此被描述为在步骤 S63 之前，但它们的执行顺序可以颠倒过来，或者并行地执行。

[0082] 选择 G、m、x 和 g 后，在控制单元 55 的控制下，选择一个满足 $0 < |r| < m$ 的整数 r 作为所述指示符，以产生新的公钥（步骤 S64）。

[0083] 选择了 G、m、x、g 和 r 后，通过计算 $y_1 = g^r$ 和 $y_2 = y_1^x$ 来产生新的公钥（步骤 S65）。然后可向接收者公开公钥 (y_1, y_2) 以用于加密（步骤 S66）。当然，可以有其他信息与所述公钥一起公开。

[0084] 应注意，g、x 和 r 的选择彼此之间没有顺序和依赖性需求，因此步骤 S62、S63 和 S64 可以任何顺序执行，不论是串行还是并行。另外，g、x 和 r 的选择可以是随机的，也可以根据所需的标准进行。

[0085] 或者，前述步骤中的一些可被控制单元 55 省略，而在其他地方执行。例如，群 G 和所述子群可由第三方例如信托机构指定。因此，控制单元 55 就跳过了选择群和子群的步骤，因为它们在外部被确定。而且，如果以前已产生过一个匿名公钥，则肯定已选择并确定了所述群、子群、生成子和私钥。因此当要产生新的公钥时，控制单元 55 就跳过这 4 个步骤而直接进行到后续步骤。

[0086] 如果 y_1 或 y_2 原来位于群 G 的范围之外，则它们必须被映射到群 G 内。映射方法可根据不同的群而不同。然而，循环群 G 确保了这种映射方法的存在。

[0087] 应注意，前述步骤或者可以在系统的单个设备 / 模块执行（利用集成或分离的组件），也可以分布式的方式进行，其中系统的不同设备分别执行这些步骤中的一些步骤。

[0088] 选择群、子群和生成子的示例

[0089] 下面描述了群、子群和生成子选择的示例。假设选择了群 Z_p^*，其中 p = 11，因此 Z_{11}^* = {1,2,3,4,5,6,7,8,9,10}。由于 11 是素数，因此数学上 Z_{11}^* 的阶数是 11-1 = 10。元素 2 是 Z_{11}^* 的生成子，因为可容易地验证 $Z_{11}^* = \{2^i \bmod 11 / i = 0,1, \cdots,9\}$。由于群是它自身的子群，所述子群可被选择为 Z_{11}^*。子群的另一个选择例如是 {1,3,4,5,9}，阶数为 5，具有生成子 3。也很容易地可验证 $3^5 = 1 \bmod 11$。

[0090] 而且，如本领域内的技术人员可认识到的那样，所有所述设备和组件都可实现为硬件、软件、固件或其组合，根据不同的考虑而各异。

[0091] 密钥产生的优化

[0092] 基本上是在图 6 中描述的示例性方法只是可用于产生根据本发明的匿名公钥的许多方法中的一种。还存在更高级的方法，不仅可用于相同的目的，还可获得性能上的优化。为描述这些优化方法，下面参考图 4、5 和 7 简单地总结本领域内公知的编码和解码过程，其中⊙是群 G 上的可逆运算，⊘是⊙的逆运算。已将本发明应用到图 7 中的过程中。

[0093] 为了加密明文 M，首先将 M 表示为 G 的元素（例如将 M 表示为 ASCII 码）（步骤 S80），然后选择满足 $1 < |k| < m$ 的一个整数 k 作为指定符（步骤 S81），并如下计算一对值（步骤 S82）

[0094] $C_1 = y_1^k$ 和

[0095] $C_2 = M \odot y_2^k$

[0096] 其中 C_1 和 C_2 和群 G 的元素。所有这些操作都可由图 4 中的编码设备 48 完成。⊙的示例可以是群 G 上的乘法、除法、加法或减法。如果 C_1 和 C_2 原来位于群 G 的范围之外，则它们必须被映射到群 G 内。映射方法根据不同的群而不同。

[0097] 此时，获得了消息 M 的密文 $C = (C_1, C_2)$（步骤 S83），并可由发送单元 44 通过通信信道向外发送。

[0098] 对于位于群 G 的范围之外的将要编码的消息 M，在编码前它必须被转换成若干群元素。在接下来的解码之后，所恢复出的群元素必须被转换回到初始的消息。转换方法可根据不同的群而不同。一个示例是将消息分割成若干块，每个块都是群 G 的元素，并串接所有的块来重构 M。

[0099] 在通信信道的另一侧，接收到密文消息 C（步骤 S84）。为了从密文 C 获取明文 M，首先必须在两种方式之间作出决定，即是否进行直接指数运算（步骤 S85）。如果是，则首先计算 $rb = C_1^x$（步骤 S86），然后通过计算 $M = C_2 \oslash rb$ 来获得 M（步骤 S87）；否则就首先计算 $ra = C_1^{-x}$（步骤 S88），然后通过计算 $M = C_2 \odot ra$ 来获得 M（步骤 S89）。

[0100] 在成功地解密密文 (C_1, C_2) 后，根据解密的实现方式，公钥产生设备 49 根据本发明可利用所接收的密文以及中间解密输出 ra 来产生新的匿名公钥，其形式为 $(y_1 = C_1^{-1}, y_2 = ra)$。类似地，公钥产生设备 49 可利用所接收的密文以及中间解密输出 rb 来产生新的匿名公钥，其形式为 $(y_1 = C_1, y_2 = rb)$。在这两种产生新的匿名公钥的方法中，都可避免指数运算，提高了计算效率。

[0101] 而且，当提供了单个匿名公钥 (y_1, y_2) 时，公钥产生设备 49 可产生一个新的匿名公钥，形式为 (y_2, y_2^x)。这一方法可被使用多次以产生一系列公钥。按照这种方式，所产生的公钥的存储消耗可被大大减少，因为公钥第二部分 y_2 与其后续结果的第一部分相同。对于

一系列 w 个公钥，最多可节省百分比为 (w-1)/2w 的存储，也就意味着对于足够大的 w 来说，几乎节省了 50％。

[0102] 在本发明中，由于公钥是基于生成子的幂的形式，利用同一个生成子来产生的，因此生成子 g 的幂可被重复使用于产生一系列公钥，这涉及的是乘法而不是指数运算，因而节省了存储器并加速了计算。同时，由于在解码设备中只需要维护一张生成子的幂表，因此可以离线执行新公钥的计算。

[0103] 例如，在一个实施例中，当在解码设备中接收到密文消息 $C = (C_1, C_2)$ 时，可获取 C 并用来产生新的公钥。如前所述，$C_1 = y_1^k = g^{rk}$，并且 g^{rk} 可被保存来产生新的公钥，因为乘积“rk”只是另一个整数。应注意，尽管 g^{rk} 可被保存来产生新的公钥，但是 rk 的值对于解码设备来说可能仍然是未知的，除非编码设备在发送加密消息时公开了 k。

[0104] 当提供了单个匿名公钥 (y_1, y_2) 时，公钥产生设备 49 可产生一个新的匿名公钥，形式为 $(y_1 \times y_1, y_2 \times y_2)$，其中 × 是群乘法。一般地，如果提供了若干匿名公钥 (y_{11}, y_{21})、(y_{12}, y_{22})、…、(y_{1j}, y_{2j})，$j \geq 2$，则基于所存储的多个 g 的幂 $y_{11} = g^{r1}$、$y_{12} = g^{r2}$、…、$y_{1j} = g^{rj}$，以及 $y_{21} = y_{11}^x$、$y_{22} = y_{12}^x$、…、$y_{2j} = y_{1j}^x$，可以计算一个新的公钥为 $(y_{1(j+1)} = y_{11}y_{12}\cdots y_{1j}$，$y_{2(i+1)} = y_{21}y_{22}\cdots y_{2j})$，其中 $y_{11}y_{12}\cdots y_{1j}$ 是 y_{11}、$y_{12}\cdots y_{1j}$，的乘积，$y_{21}y_{22}\cdots y_{2j}$ 是 y_{21}，、y_{22}、…、y_{2j} 的乘积。很清楚，为了产生新的匿名公钥，指数运算被乘法所取代，提高了计算效率。由于可以在线执行乘法，因此按照这种方式产生的新公钥不必被预先计算，这直接意味着存储空间的节省。

[0105] 上述优化技术可结合起来使用以产生新的匿名公钥。例如，在接收并成功地解密一系列密文 (C_{11}, C_{21})、(C_{12}, C_{22})、…、(C_{1j}, C_{2j})，$j \geq 2$ 后，公钥产生设备 49 可利用所接收的密文以及中间解密输出 rb_1、rb_2、…、rb_j 来产生一个新的匿名公钥，形式为 $(y_1 = (C_{11}C_{12}\cdots C_{1j})$，$y_2 = (rb_1rb_2\cdots rb_j))$，其中 $C_{11}C_{12}\cdots C_{1j}$i 是 C_{11}、C_{12}、…、C_{1j} 的乘积，$rb_1rb_2\cdots rb_j$ 是 rb_1、rb_2、…、rb_j 的乘积。

[0106] 而且，利用对 y_2 的计算，可以计算一系列公钥 (y_2^{W1}, y_2^{W2})，其中 $w_1 = x^w$，$w_2 = x^{(w+1)}$，$w \geq 0$。而且，这一计算中获得的所有结果，尤其是 g 的幂，都可利用来产生其他公钥。

[0107] 而且，基于从密文 C 获取的 C_1，解码设备可以产生更多的新公钥。为此，计算并保存 C_1^x 和 C_1^{-x}，然后可以产生两个系列的公钥。一般地，当接收到多个加密消息 $CC_1 = (C_{11}, C_{12})$、$CC_2 = (C_{21}, C_{22})$、…、$CC_j = (C_{j1}, C_{j2})$，$j \geq 1$ 时，对于 C_1^x，可以产生一系列的公钥 $((C_{11}C_{21}\cdots C_{j1})^{u1}$，$(C_{11}C_{21}\cdots C_{j1})^{u2})$，其中 $C_{11}C_{21}\cdots C_{j1}$ 是 C_{11}、C_{21}、…、C_{j1} 的乘积，$u1 = x^u$，$u2 = x^{(u+1)}$ 并且 $u \geq 0$，对于 C_1^{-x}，可以产生另一系列的公钥 $((C_{11}C_{21}\cdots C_{j1})^{v1}$，$(C_{11}C_{21}\cdots C_{j1})^{v2})$，其中 $C_{11}C_{21}\cdots C_{j1}$ 是 C_{11}、C_{21}、…、C_{j1} 的乘积，$v1 = -x^v$，$v2 = -x^{(v+1)}$ 并且 $v \geq 0$。而且，这一计算中获得的所有结果，尤其是 g 的幂，都可被利用来产生其他公钥。

[0108] 匿名私钥

[0109] 在一些情形下，用户可能希望选择若干私钥，并分别为不同的私钥产生若干系列的匿名公钥。用户可选择若干私钥 x_i，并为每个私钥 x_i 产生匿名公钥 (g^a, g^{axi})。由于“一公钥对一私钥”模型被本发明的教导所取代，因此匿名公钥的匿名性也就隐含着所述若干私钥的匿名性。在此意义上，本发明还实现了匿名私钥。

[0110] 安全通信会话的示例

[0111] 下面将示出一个根据本发明的安全通信会话实施例，其中的匿名公钥技术基于循

环群 Z_p^*。为了简单，p = 11，因此 Z_{11}^* = {1,2,3,4,5,6,7,8,9,10}。Z_{11}^* 的阶数是 10。子群被选择为 Z_{11}^*。生成子是 2。

[0112] 在解密侧，私钥被选择为 x = 3。如果整数 a = 4 被选择为指示符，则公钥产生设备 49 产生匿名公钥 $(2^4 = 5, 5^3 = 4) \bmod 11$。对于另一个整数 a = 7，公钥产生设备 49 产生另一个匿名公钥 $(2^7 = 7, 7^3 = 2) \bmod 11$。

[0113] 假设着两个匿名公钥被传递给两个接收者。接收了公钥 (5,4) 的接收者 A 要加密明文 8。另一个接收者 B 要加密明文 10。

[0114] 接收者 A 选择整数 6 作为指定符，并计算 8 的密文 $(5^6 = 5, 8 \times 4^6 = 10) \bmod 11$。类似地，接收者 B 选择整数 3 并计算 10 的密文 $(7^3 = 2, 10 \times 2^3 = 3) \bmod 11$。

[0115] 密文 (5,10) 和 (2,3) 被分别传递给解码侧。(5,10) 的明文可根据 $5^{-3} = 5^{10} \times 5^{-3} = 5^7 = 3 \bmod 11$ 和 $10 \times 3 = 8 \bmod 11$ 来计算。(2,3) 的明文可根据 $2^3 = 8 \bmod 11$ 和 $3/8 = 3 \times 8^{-1} = 3 \times 8^{10} \times 8^{-1} = 3 \times 8^9 = 10 \bmod 11$ 来计算。

[0116] 这样就在解码侧成功的获取了明文 8 和 10。而且，可以利用优化技术来产生新的匿名公钥。

[0117] 基于密文 (2,3) 和中间解码输出 8，可以产生一个匿名公钥 (2,8) 。

[0118] 基于密文 (5,10) 和中间解码输出 3，可以产生一个匿名公钥 $(5^{-1} = 9, 3) \bmod 11$。

[0119] 基于一个匿名公钥 (2,8)，可以产生一系列公钥 (2,8)、$(8, 8^3 = 6)$、$(6, 6^3 = 7) \bmod 11$。

[0120] 基于一个匿名公钥 (9,3)，可以产生一个新公钥 $(9 \times 9 = 4, 3 \times 3 = 9) \bmod 11$。

[0121] 基于所述匿名公钥中的一些，例如 (2,8) 和 (7,2)，可以产生新公钥 $(2 \times 7 = 3, 8 \times 2 = 5) \bmod 11$。

[0122] 从上述描述可以看出来自不同发送者的参数被利用来产生新的公钥。因此，可以改进所得到的公钥的隐私度。应注意，所有这些公钥都是基于单个私钥 x 和相同生成子 g 产生的。

[0123] 本发明的多个方面可以包含在计算机可读介质中的计算机可执行指令来实现，它也可以硬布线逻辑 / 电路或硬件和软件的结合来实现。而且，本说明书中所涉及的设备可包括存储器例如 RAM、DRAM 或 ROM 来存储必须的数据和计算机可执行指令，以执行本发明中所教导的步骤。并且所述存储器可被包含在所述终端的编码设备和 / 或解码设备中。存储器的这种使用方式在本领域中是公知的，因此未在此描述也未在附图中示出。

[0124] 本发明可被体现为其他形式，而不偏离其精神和实质特性。因此，所提供的实施例在任何情况下都应看作为说明性而非限制性的，本发明的范围由所附权利要求指明，而非由前述说明确定，并且处于所述权利要求的意义和等同范围内的所有改变也应被包含于其中。

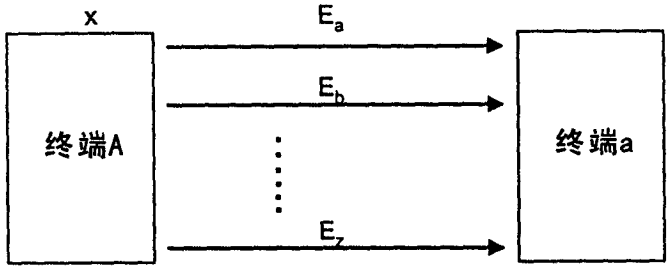


图1

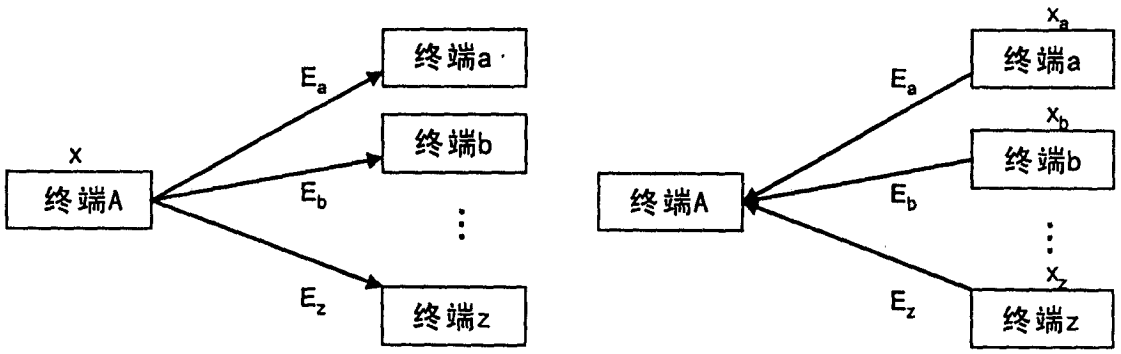


图2

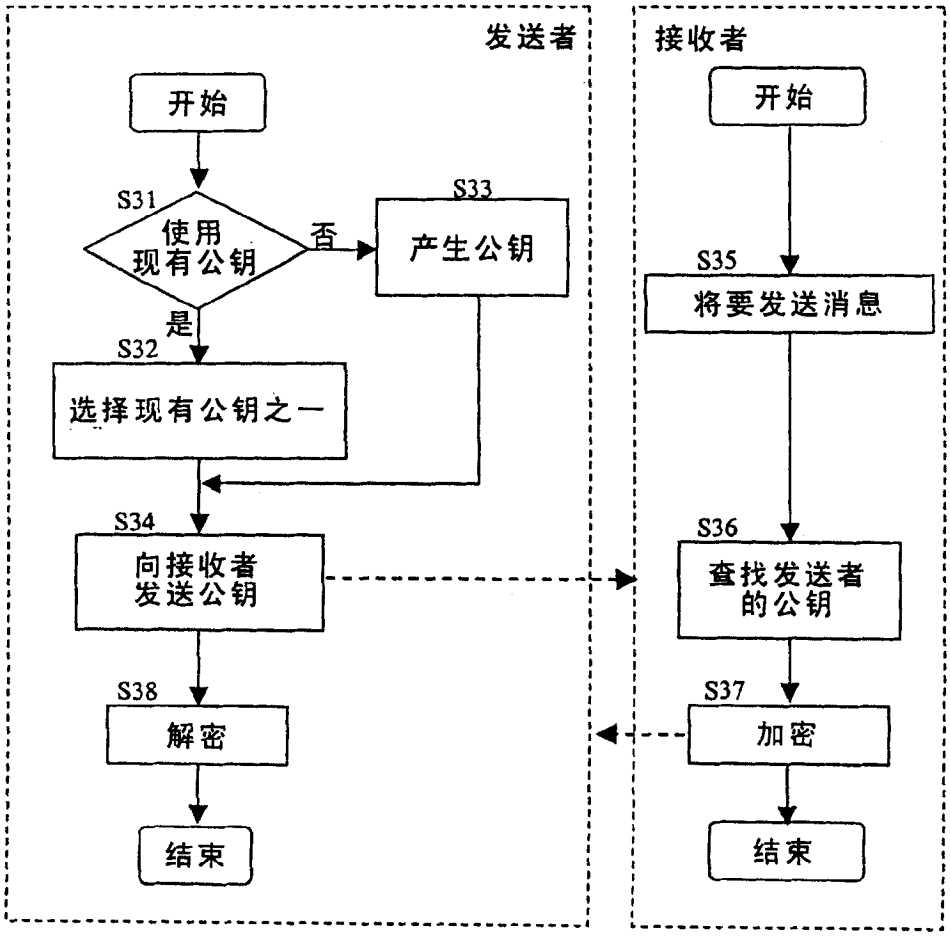

发送者
开始
S31
使用现有公钥
否
S33
产生公钥
是
S32
选择现有公钥之一
S34
向接收者发送公钥
S38
解密
结束
接收者
开始
S35
将要发送消息
S36
查找发送者的公钥
S37
加密
结束

图3

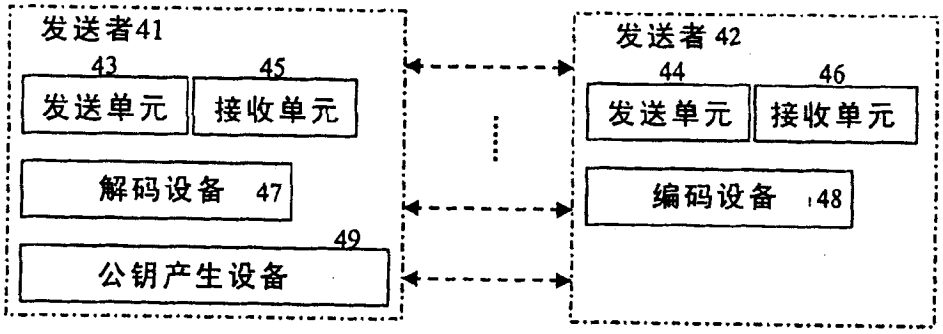

发送者41
43
发送单元
45
接收单元
解码设备 47
49
公钥产生设备
发送者 42
44
发送单元
46
接收单元
编码设备 48

图4

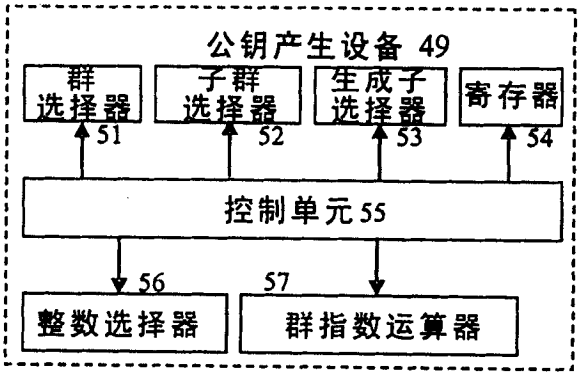

公钥产生设备 49
群选择器
51
子群选择器
52
生成子选择器
53
寄存器
54
控制单元 55
56
57
整数选择器
群指数运算器

图5

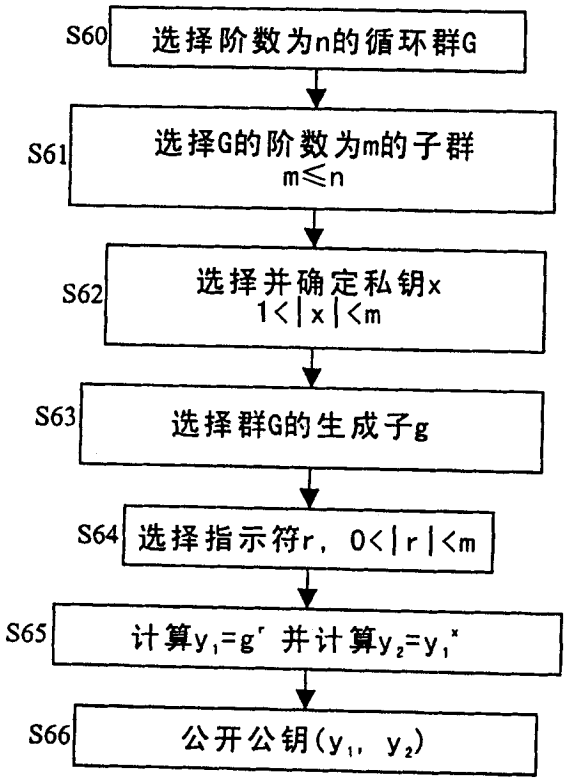

S60
选择阶数为n的循环群G
S61
选择G的阶数为m的子群
m≤n
S62
选择并确定私钥x
1<|x|<m
S63
选择群G的生成子g
S64
选择指示符r，0<|r|<m
S65
计算$y_1=g^r$ 并计算$y_2=y_1^x$
S66
公开公钥(y_1，y_2)

图6

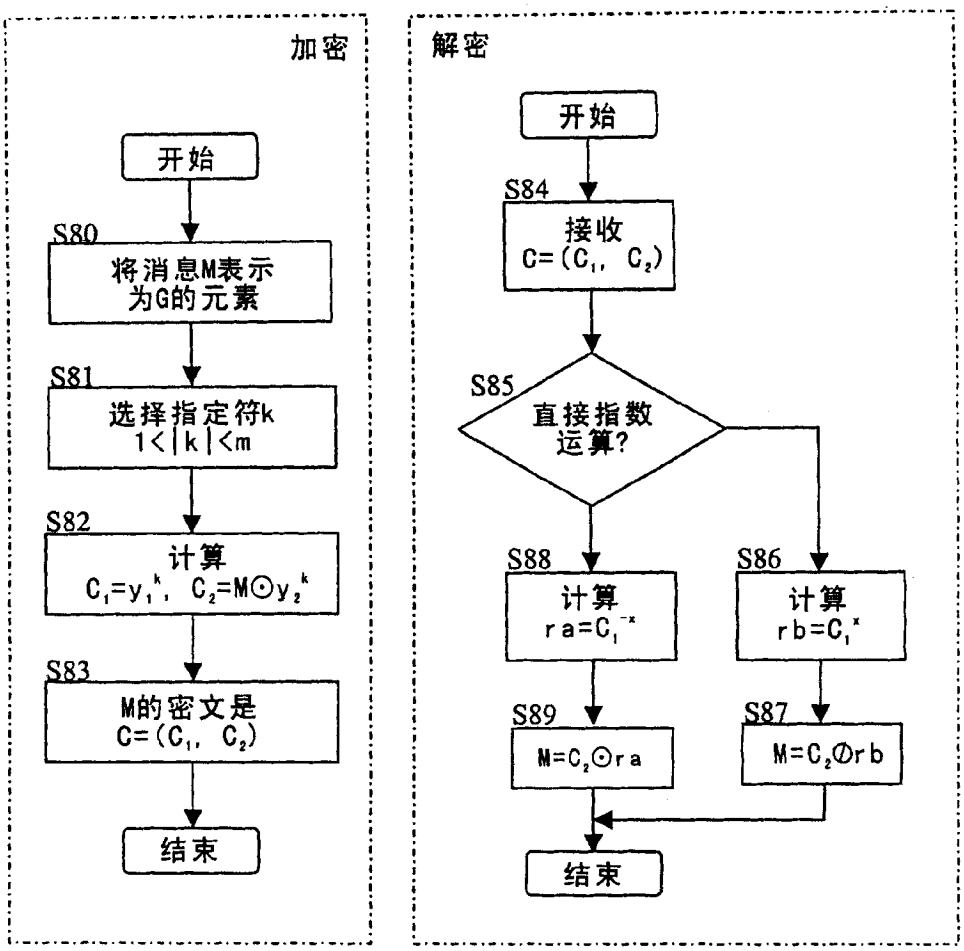

加密
开始
S80
将消息M表示为G的元素
S81
选择指定符k
1<|k|<m
S82
计算
C1=y1^k, C2=M⊙y2^k
S83
M的密文是
C=(C1, C2)
结束
解密
开始
S84
接收
C=(C1, C2)
S85
直接指数运算?
S88
计算
ra=C1^-x
S86
计算
rb=C1^x
S89
M=C2⊙ra
S87
M=C2⊘rb
结束

图7