

## (12) 发明专利

(10) 授权公告号 CN 1993922 B

(45) 授权公告日 2012.11.14

(21) 申请号 200580025880.7

H04L 9/18(2006.01)

(22) 申请日 2005.07.15

(56) 对比文件

(30) 优先权数据

US 2004/071289 A1, 2004.04.15, 全文.

10/909,004 2004.07.30 US

US 2003/0086564 A1, 2003.05.08, 全文.

(85) PCT申请进入国家阶段日

GB 2353191 A, 2001.02.14, 全文.

2007.01.30

审查员 薛玮

(86) PCT申请的申请数据

PCT/US2005/025338 2005.07.15

(87) PCT申请的公布数据

W02006/012363 EN 2006.02.02

(73) 专利权人 英特尔公司

地址 美国加利福尼亚州

(72) 发明人 G·L·格劳恩克

(74) 专利代理机构 中国专利代理(香港)有限公司 72001

代理人 程天正 梁永

(51) Int. Cl.

H04L 9/06(2006.01)

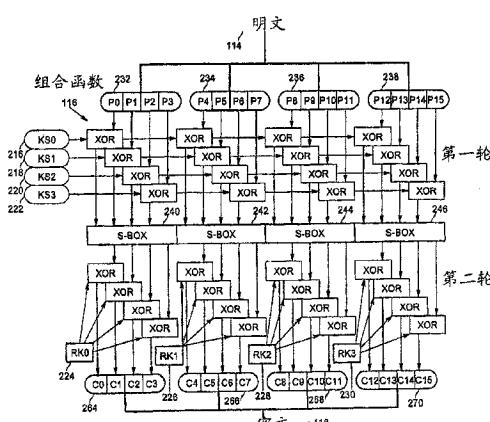
权利要求书 3 页 说明书 5 页 附图 4 页

(54) 发明名称

流密码组合系统和方法

(57) 摘要

一种加密系统及方法，包括：从密钥流分组中产生多个轮密钥；以及执行组合函数。在将一组明文数据分组加密成一组密文数据分组时，该组之内的每个明文数据分组利用所选密钥流分组和所选轮密钥的唯一组合进行处理，而且密钥流的大小小于明文数据的大小。在将一组密文数据分组解密成一组明文数据分组时，该组之内的每个密文数据分组利用所选密钥流分组和所选轮密钥的唯一组合进行处理，而且密钥流的大小小于密文数据的大小。



1. 一种加密系统,包括:

至少部分地基于密钥和初始化向量产生密钥流的密钥流发生器;

至少部分地基于密钥流产生多个轮密钥的轮密钥发生器;以及

至少部分地基于同样大小的一组明文数据分组、密钥流和轮密钥来产生一组密文数据分组的组合函数装置,所述组合函数装置包括:第一轮代数函数装置,利用多个密钥流分组对明文数据分组进行运算,以产生第一中间结果;多个非线性变换函数装置,对第一中间结果进行运算以产生第二中间结果;以及第二轮代数函数装置,利用轮密钥对第二中间结果进行运算,以产生密文数据。

2. 如权利要求1所述的加密系统,其中,所述组之内的每个明文数据分组通过所述组合函数装置利用所选密钥流分组和所选轮密钥的唯一组合进行处理。

3. 如权利要求1所述的加密系统,其中,每个非线性变换函数装置包括置换盒(S-box)装置。

4. 如权利要求1所述的加密系统,其中,所述密钥流的大小小于明文数据的大小。

5. 如权利要求1所述的加密系统,其中,密钥流分组的数目等于轮密钥的数目。

6. 如权利要求1所述的加密系统,其中第一轮代数函数装置包括多个异或(XOR)函数装置。

7. 如权利要求1所述的加密系统,其中,第一轮的每个代数函数装置接受明文数据分组和密钥流分组作为输入,以产生第一中间结果分组。

8. 如权利要求1所述的加密系统,其中,第二轮代数函数装置包括多个异或(XOR)函数装置。

9. 如权利要求1所述的加密系统,其中,第二轮的每个代数函数装置接受第二中间结果分组和一个轮密钥作为输入,以产生密文数据分组。

10. 如权利要求1所述的加密系统,其中,所述组明文数据分组之内的每个明文数据分组通过组合函数装置基本上与所述组的所有其他分组并行进行处理,以产生密文数据。

11. 一种加密数据的方法,包括:

至少部分地基于初始化向量和密钥产生多个密钥流分组;

产生多个轮密钥,每个轮密钥至少部分地基于密钥流分组;

通过以下步骤从一组明文数据分组中产生一组密文数据分组:

对每个明文数据分组和所选密钥流分组执行第一轮代数函数,以产生第一中间结果;

对第一中间结果执行非线性变换,以产生第二中间结果;以及

对第二中间结果的每个分组和所选轮密钥执行第二轮代数函数,以产生每个密文数据分组。

12. 如权利要求11所述的方法,其中,所述组之内的每个明文数据分组利用所选密钥流分组和所选轮密钥的唯一组合进行处理。

13. 如权利要求11所述的方法,其中,所述密钥流的大小小于明文数据的大小。

14. 如权利要求13所述的方法,其中,密钥流分组的数目等于轮密钥的数目。

15. 如权利要求11所述的方法,其中,执行第一轮代数函数包括执行多个异或(XOR)函数。

16. 如权利要求11所述的方法,其中,执行第二轮代数函数包括执行多个异或(XOR)函

数。

17. 如权利要求 11 所述的方法,其中,所述组明文数据分组之内的每个明文数据分组基本上与所述组的所有其他分组并行进行处理,以产生密文数据。

18. 一种从一组明文数据分组中产生一组密文数据分组的方法,包括:

对每个明文数据分组和所选密钥流分组执行第一代数函数,以产生第一中间结果;

对第一中间结果执行非线性变换,以产生第二中间结果;以及

对每个第二中间结果分组和所选轮密钥执行第二代数函数,以产生每个密文数据分组,所述所选轮密钥至少部分地从密钥流中产生。

19. 如权利要求 18 所述的方法,其中,所述组之内的每个明文数据分组利用所选密钥流分组和所选轮密钥的唯一组合进行处理。

20. 如权利要求 18 所述的方法,其中,所述密钥流的大小小于明文数据的大小。

21. 如权利要求 18 所述的方法,其中,所述组明文数据分组之内的每个明文数据分组基本上与所述组的所有其他分组并行进行处理,以产生密文数据。

22. 一种加密数据的方法,包括:

从密钥流分组中产生多个轮密钥;以及

将一组明文数据分组加密成一组密文数据分组,其中,所述组之内的每个明文数据分组利用所选密钥流分组和所选轮密钥的唯一组合进行处理,而且密钥流的大小小于明文数据的大小。

23. 如权利要求 22 所述的方法,其中,所述组明文数据分组之内的每个明文数据分组基本上与所述组的所有其他分组并行进行处理,以产生密文数据。

24. 一种解密系统,包括:

至少部分地基于密钥和初始化向量产生密钥流的密钥流发生器;

至少部分地基于密钥流产生多个轮密钥的轮密钥发生器;以及

至少部分地基于同样大小的一组密文数据分组、密钥流和轮密钥来产生一组明文数据分组的组合函数装置,所述组合函数装置包括:第一轮代数函数装置,利用轮密钥对密文数据分组进行运算,以产生第一中间结果;多个非线性逆变换函数装置,对第一中间结果进行运算,以产生第二中间结果;以及第二轮代数函数装置,利用多个密钥流分组对第二中间结果进行运算,以产生明文数据。

25. 如权利要求 24 所述的解密系统,其中,所述组之内的每个密文数据分组通过组合函数装置利用所选密钥流分组和所选轮密钥的唯一组合进行处理。

26. 如权利要求 24 所述的解密系统,其中,所述密钥流的大小小于密文数据的大小。

27. 如权利要求 24 所述的解密系统,其中,密钥流分组的数目等于轮密钥的数目。

28. 如权利要求 24 所述的解密系统,其中,第一轮代数函数装置和第二轮代数函数装置的至少之一包括多个异或(XOR) 函数装置。

29. 如权利要求 24 所述的解密系统,其中,第一轮的每个代数函数装置接受密文数据分组和所选轮密钥作为输入,以产生第一中间结果分组。

30. 如权利要求 24 所述的解密系统,其中,第二轮的每个代数函数装置接受第二中间结果分组和所选密钥流分组作为输入,以产生明文数据分组。

31. 如权利要求 24 所述的解密系统,其中,所述组密文数据分组之内的每个密文数据

分组通过组合函数装置基本上与所述组的所有其他分组并行进行处理,以产生明文数据。

32. 一种解密数据的方法,包括:

至少部分地基于初始化向量和密钥产生多个密钥流分组;

产生多个轮密钥,每个轮密钥至少部分地基于密钥流分组;

通过下列步骤从一组密文数据分组中产生一组明文数据分组:

对每个密文数据分组和所选轮密钥执行第一轮代数函数,以产生第一中间结果;

对第一中间结果执行非线性逆变换,以产生第二中间结果;以及

对每个第二中间结果分组和所选密钥流分组执行第二轮代数函数,以产生每个明文数据分组。

33. 如权利要求 32 所述的方法,其中,所述组之内的每个密文数据分组利用所选密钥流分组和所选轮密钥的唯一组合进行处理。

34. 如权利要求 32 所述的方法,其中,所述密钥流的大小小于密文数据的大小。

35. 如权利要求 32 所述的方法,其中,密钥流分组的数目等于轮密钥的数目。

36. 如权利要求 32 所述的方法,其中,执行第一轮代数函数和第二轮代数函数的至少之一包括执行多个异或 (XOR) 函数。

37. 如权利要求 32 所述的方法,其中,所述组密文数据分组之内的每个密文数据分组基本上与所述组的所有其他分组并行进行处理,以产生明文数据。

38. 一种从一组密文数据分组中产生一组明文数据分组的方法,包括:

对每个密文数据分组和所选轮密钥执行第一代数函数,以产生第一中间结果;

对第一中间结果执行非线性逆变换,以产生第二中间结果;以及

对每个第二中间结果分组和所选密钥流分组执行第二代数函数,以产生每个明文数据分组,所述所选轮密钥至少部分地从密钥流中产生。

39. 如权利要求 38 所述的方法,其中,所述组之内的每个密文数据分组利用所选密钥流分组和所选轮密钥的唯一组合进行处理。

40. 如权利要求 38 所述的方法,其中,所述密钥流的大小小于密文数据的大小。

41. 如权利要求 38 所述的方法,其中,所述组密文数据分组之内的每个密文数据分组基本上与所述组的所有其他分组并行进行处理,以产生明文数据。

42. 一种解密数据的方法,包括:

从密钥流分组中产生多个轮密钥;以及

将一组密文数据分组解密成一组明文数据分组,其中,所述组之内的每个密文数据分组利用所选密钥流分组和所选轮密钥的唯一组合进行处理,而且密钥流的大小小于密文数据的大小。

43. 如权利要求 42 所述的方法,其中,所述组密文数据分组之内的每个密文数据分组基本上与所述组的所有其他分组并行进行处理,以产生明文数据。

## 流密码组合系统和方法

[0001] 背景

[0002] 1. 领域

[0003] 本发明总的涉及密码学,更具体而言,涉及流密码和组合函数。

[0004] 2. 说明

[0005] 在某些情况下,密码系统被用于保护未压缩的视频数据。因为视频数据是未被压缩的,所以为了向用户显示而要处理的数据量非常大。通常,例如利用诸如高级加密标准(AES)密码之类的已知分组密码来加密此数据,对于某些内容保护应用是非常慢的。

[0006] 在典型的流密码加密运算中,通过利用简单的组合运算,例如异或,把密钥流直接施加到明文数据以产生密文数据。反之,在解密运算期间,使用相同的密钥流和逆向的组合运算来将密文数据改变回明文数据。此方法的一个缺点在于,它需要与将要处理的数据相同的密钥流比特量。

[0007] 所希望的是一种密码系统,该密码系统使用小于明文数据大小的密钥流,从而改进密码系统的性能特征,但依然提供足够的安全性。

### 附图说明

[0008] 本发明的特征和优点将从下列本发明的详细说明中变得清晰可见,其中:

[0009] 图1是根据本发明实施例的密码系统的高级框图;

[0010] 图2是根据本发明实施例图示密码系统的密钥产生处理的框图;

[0011] 图3是根据本发明实施例图示供密码系统加密使用的组合函数处理的框图;

[0012] 图4是根据本发明实施例图示供密码系统解密用的组合函处理的框图。

[0013] 详细说明

[0014] 本发明的实施例是用于通过将密钥流部分用作以一轮一次分组密码形式的轮密钥来改进流密码性能的方法和设备。这允许在保持所希望的安全特性的同时,以相同的时间量加密或解密更多的数据。

[0015] 在本发明的实施例中,少量的密钥流分组可以按照对于根流密码(base steam cipher)所典型计算的方式那样来计算,但是此密钥流的分组现在可以用作短分组密码形式的轮密钥,密钥流分组的每个组合至多一次被用作这些轮密钥的根(basis)。在一个实施例中,为了在一些明文数据分组被得知(因此可能导出附近的未知明文分组)的情况下,阻止敌手解得密钥流,可以在组合运算之间使用诸如置换盒(S-box)之类的非线性变换。短分组密码可以将来自多个分组中每一分组的对应位用作置换运算的输入数据,并且多个分组可以一起被加密或解密。在一个实施例中,可以对密钥流位做移位或其他变换,以便从该密钥流的初始分组中形成后续的轮密钥(round key)。

[0016] 说明书中对本发明“一个实施例”或“一实施例”的引用意欲将结合实施例描述的具体特征、结构或特性归入本发明的至少一个实施例中。因此,出现在说明书各个地方的词组“在一个实施例中”不一定都是指相同的实施例。

[0017] 图1是根据本发明实施例的密码系统100的高级框图。在该系统中,初始化向量

(IV) 102 和密钥 104 可被输入至密钥流发生器 106。初始化向量包括多个随机或伪随机产生的位。在一个实施例中，IV 可以包括四个分组，其中，IV 的每个分组中的位数可以是 128，不过在其他的实施例中，可以使用其他大小和数量的分组。密钥 104 可以是任何位序列。在一个实施例中，密钥是保密的。在一个实施例中，密钥中的位数可以是 128；而在其他的实施例中，可以使用其他的大小。密钥流发生器 106 接受密钥和 IV，并产生密钥流 108。在一个实施例中，密钥流发生器根据本领域技术人员公知的方法，通过在计数器模式 (CTR) 或者输出反馈模式 (OFB) 下利用已知的分组密码运算，基于输入数据产生密钥流。在一个实施例中，密钥流发生器使用 AES 密码。在其他的实施例中，可以采用其他公知的分组密码。在更进一步的实施例中，流密码（例如，RC4）可以用作密钥流发生器来代替分组密码。通常，密钥流可以是任何任意长度的位。在本发明的实施例中，密钥流包括数量小于明文 114 中的位数的位，所以改进了组合函数 116 的总性能。

[0018] 在一实施例中，可以向轮密钥发生器 110 和组合函数 116 都输入密钥流 108。轮密钥发生器使用密钥流的分组来产生多个轮密钥。在一个实施例中，轮密钥可以通过每次对该密钥流的 4 个分组进行运算，按照 4 个一组的方式来产生（其中，在一个实施例中，每个分组包括 128 位）。在一实施例中，轮密钥发生器可以包括逻辑函数，例如移位函数（左移或右移规定的位数）。在其他的实施例中，可以对密钥流分组执行其他的逻辑函数来产生轮密钥。轮密钥 112 可以是任意的适宜大小。在一个实施例中，每个轮密钥可以包括 128 位。

[0019] 在如图 1 所示的一个实施例中，组合函数 116 可以使用轮密钥 112 和密钥流 108 来将明文 114 加密成密文 118。可替换地，可以使用具有逆向数学特性的组合函数来利用轮密钥和密钥流执行把密文 118 还原成明文 114 的解密。因为在本发明的实施例中，密钥流小于明文，所以与现有技术方法相比，本发明的密码能够更快速地产生密文。

[0020] 图 2 是根据本发明实施例图示密码系统的密钥产生过程的框图。此图图示了图 1 所示的实施例的方框 106 ~ 112 的附加细节。密钥 104 和 IV 102 可以被输入至密钥流发生器 106。IV 可以被编组成四个分组，标记为 IV\_200, IV\_1202, IV\_2204, 和 IV\_3206。在一个实施例中，每个 IV 分组包括 128 位。在其他的实施例中，可以采用其他的大小。每个 IV 分组可以被输入至分组密码。在一个实施例中，分组密码可以是 AES。例如，如图 2 所示，第一分组 IV\_200 可以被输入至第一 AES\_208，第二分组 IV\_1202 可以被输入至第二 AES\_210，第三分组 IV\_2204 可以被输入至第三 AES\_212，以及第四分组 IV\_3206 可以被输入至第四 AES\_214。每个 AES 密码可以在计数器 (CTR) 模式下使用，例如用以基于选择的 IV 分组和密钥来产生密钥流分组。在对一组四个分组运算（在一个实施例中）时，AES 密码分别产生密钥流 0 (KS0)\_216、密钥流 1 (KS1)\_218、密钥流 2 (KS2)\_220 和密钥流 3 (KS3)\_222 的分组。可以操作密钥流发生器以随着时间的过去而产生连续多组的四个密钥流分组。密钥流分组可以被输入至多个轮密钥发生器 (RKG) 250, 252, 254, 256，如图所示。每个 RKG 使用作为输入接收的密钥流分组，并生成轮密钥。当在一个迭代中对一组四个分组进行运算时（在一个实施例中），这组的四个 RKG\_250, 252, 254, 256 分别产生轮密钥 RK0\_224, RK1\_226, RK2\_228, RK3\_230。在一个实施例中，每个轮密钥可以是 128 位，不过可以使用其他的大小。产生密钥流分组和轮密钥的每个路径可以并行执行。在一实施例中，四个 RKG 可以被组合成一个实体，用以同时为所有四个分组执行轮密钥生成函数。

[0021] 密钥流发生器和轮密钥发生器迭代一次的处理结果是一组四个密钥流分组 (KS0、

KS1、KS2、和 KS3) 和四个轮密钥 (RK0、RK1、RK2、和 RK3)，它们是从初始密钥 104 和初始化向量分组 200、202、204、206 中导出的。在本发明的实施例中，一个密钥流分组和轮密钥对的每种唯一组合 (例如 (KS0, RK0)、(KS0, RK1)、… (KS3, RK2)、(KS3, RK3)) 可以在组合函数 116 的两轮中被用作密钥，以便从 16 个明文分组中产生 16 个密文分组。因此，在本发明的实施例中，只使用 4 个密钥流数据分组，就可以对 16 个数据分组执行加密或解密运算。这导致比现有技术系统高达四倍的处理改进。

[0022] 此性能改善可以按如下获得。图 3 是根据本发明实施例说明用于加密的组合函数处理的框图。通常，组合函数包括两轮和一组 S-box 变换。可以将明文 114 输入组合函数 116。将明文连同所选密钥流分组一起输入第一轮可逆代数函数，以产生第一中间结果。第一中间结果被发送给一组四个的 S-box。S-box 产生第二中间结果。将第二中间结果连同所选轮密钥一起输入第二轮可逆代数函数。第二轮的输出包括密文 118。一组明文数据中的每个分组可通过该组合函数基本上与所有其他分组同时进行处理，以产生一组密文数据分组。

[0023] 在一个实施例中，明文数据流的每个连续的 16 个分组部分 (在组合函数每次迭代时) 可以被分成四组，每组包括四分组 :P0, P1, P2 和 P3 232 ;P4, P5, P6, 和 P7 234 ;P8, P9, P10, 和 P11 236 ;以及 P12, P13, P14, 和 P15 238；每个分组包括 128 位。因此，在一个实施例中，一组中分组的数量是 16。对于第一轮处理，可以将明文分组 P0 连同密钥流 0 (KS0) 216 一起输入可逆代数函数，例如 XOR。处理 P0 的 XOR 的输出可以转送给第一 S-box 240。可以将明文分组 P1 连同密钥流 1 (KS1) 218 一起输入可逆代数函数，例如 XOR。处理 P1 的 XOR 的输出可以转送给第一 S-box 240。可以将明文分组 P2 连同密钥流 2 (KS2) 220 一起输入可逆代数函数，例如 XOR。处理 P2 的 XOR 的输出可以转送给第一 S-box 240。可以将明文分组 P3 连同密钥流 3 (KS3) 222 一起输入可逆代数函数，例如 XOR。处理 P3 的 XOR 的输出可以转送给第一 S-box 240。

[0024] 按类似方式，可以将明文分组 P4 连同密钥流 0 (KS0) 216 一起输入可逆代数函数，例如 XOR。图 3 出于简洁，KS0 被显示为穿过 KS0 行中的每个 XOR 函数。处理 P4 的 XOR 的输出可以转送给第二 S-box 242。可以将明文分组 P5 连同密钥流 1 (KS1) 218 一起输入可逆代数函数，例如 XOR。图 3 出于简洁，KS1 被显示为穿过 KS1 行中的每个 XOR 函数。处理 P5 的 XOR 的输出可以转送给第二 S-box 242。可以将明文分组 P6 连同密钥流 2 (KS2) 220 一起输入可逆代数函数，例如 XOR。图 3 出于简洁，KS3 被显示为穿过 KS3 行中的每个 XOR 函数。处理 P6 的 XOR 的输出可以转送给第二 S-box 242。可以将明文分组 P7 连同密钥流 3 (KS3) 222 一起输入可逆代数函数，例如 XOR。图 3 出于简洁，KS3 被显示为穿过 KS3 行中的每个 XOR 函数。处理 P7 的 XOR 的输出可以转送给第二 S-box 242。

[0025] 按类似方式，可以将明文分组 P8 连同密钥流 0 (KS0) 216 一起输入可逆代数函数，例如 XOR。处理 P8 的 XOR 输出可以转送给第三 S-box 244。可以将明文分组 P9 连同密钥流 1 (KS1) 218 一起输入可逆代数函数，例如 XOR。处理 P9 的 XOR 输出可以转送给第三 S-box 244。可以将明文分组 P10 连同密钥流 2 (KS2) 220 一起输入可逆代数函数，例如 XOR。处理 P10 的 XOR 输出可以转送给第三 S-box 244。可以将明文分组 P11 连同密钥流 3 (KS3) 222 一起输入可逆代数函数，例如 XOR。处理 P11 的 XOR 输出可以转送给第三 S-box 244。

[0026] 按类似方式，可以将明文分组 P12 连同密钥流 0 (KS0) 216 一起输入可逆代数函数，

例如 XOR。处理 P12 的 XOR 输出可以转送给第四 S-box 246。可以将明文分组 P13 连同密钥流 1 (KS1) 218 一起输入可逆代数函数,例如 XOR。处理 P13 的 XOR 输出可以转送给第四 S-box 246。可以将明文分组 P14 连同密钥流 2 (KS2) 220 一起输入可逆代数函数,例如 XOR。处理 P14 的 XOR 输出可以转送给第四 S-box 246。可以将明文分组 P15 连同密钥流 3 (KS3) 222 一起输入可逆代数函数,例如 XOR。处理 P15 的 XOR 输出可以转送给第四 S-box 246。

[0027] 因此,16 个 XOR 函数中的每个 XOR 函数分别处理 16 个明文分组中的一个,并向置换盒 (S-box) 转送变换的明文数据分组。每个 S-box 240、242、244、246 包括非线性映射函数,以便将一组一起取的四个输入分组(例如,来自四个分组的 512 位) 变换成一组四个的输出分组。在此,可以使用本领域公知的任何 S-box。

[0028] 每个 S-box 的输出被输入至第二轮组合函数,其包括一组 16 个可逆代数函数,例如 XOR 函数。第一密文分组 264 可以按如下产生。通过对从第一 S-box 240 输出的第一分组和第一轮密钥 0 (RK0) 224 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C0。通过对从第一 S-box 240 输出的第二分组和 RK0 224 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C1。通过对从第一 S-box 240 输出的第三分组和 RK0 224 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C2。通过对从第一 S-box 240 输出的第四分组和 RK0 224 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C3。

[0029] 按类似方式,第二密文分组 266 可以按如下产生。通过对从第二 S-box 242 输出的第一分组和第二轮密钥 1 (RK1) 226 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C4。通过对从第二 S-box 242 输出的第二分组和 RK1 226 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C5。通过对从第二 S-box 242 输出的第三分组和 RK1 226 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C6。通过对从第二 S-box 242 输出的第四分组和 RK1 226 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C7。

[0030] 按类似方式,第三密文分组 268 可以按如下产生。通过对第三 S-box 244 输出的第一分组和第三轮密钥 2 (RK2) 228 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C8。通过对从第三 S-box 244 输出的第二分组和 RK2 228 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C9。通过对从第三 S-box 244 输出的第三分组和 RK2 228 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C10。通过对从第三 S-box 244 输出的第四分组和 RK2 228 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C11。

[0031] 按类似方式,第四密文分组 270 可以按如下产生。通过对从第四 S-box 246 输出的第一分组和第四轮密钥 3 (RK3) 230 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C12。通过对从第四 S-box 246 输出的第二分组和 RK2 230 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C13。通过对从第四 S-box 246 输出的第三分组和 RK3 230 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C14。通过对从第四 S-box 246 输出的第四分组和 RK3 230 执行诸如 XOR 之类的可逆代数函数,可以产生密文分组 C15。

[0032] 虽然在图 3 中描述了数据加密,但是本领域技术人员将意识到,数据解密可以用类似方式处理,只不过是逆运算处理。图 4 是根据本发明实施例说明用于解密的组合函数处理的框图。如图 4 所示,为了使用组合函数 117 将密文解密回明文,数据从该图的底部流向顶部以用于解密(与图 3 所示相反,数据从顶部流向底部以用于加密)。用逆运算代替 S-box,以形成逆向的 S-box 241、243、245 和 247,并且可采用本领域众所周知的所有其他

可逆代数函数的逆函数。

[0033] 在其他实施例中,可以修改图 3 和 4 所示密码系统的各种特征。例如,在一个实施例中,可以撤销 S-box。这可以以降低安全性为代价提高系统的处理速度。在一实施例中,例如,除 XOR 之外的可逆代数函数可被用于第一和第二轮,例如加法或减法。如果加法或减法被用于加密,则逆运算必须被用于解密。在另一实施例中,用于第一和第二轮的代数函数可以不同。例如,可在第一轮中使用 XOR,而在第二轮中可以使用 2 的补码加法(或反之亦然)。在又一实施例中,不同的可逆代数函数可以被用于处理同一轮中的各分组。在另一实施例中,分组的大小可以改变。

[0034] 本发明实施例的组合函数允许小常数因子用于相对于常规的流密码来改善性能(例如,高达 4 倍或高达 8 倍的改善,这取决于置换运算的细节),这是因为组合函数的计算比底层的流密码更快。

[0035] 当用软件实现时,即使采用了最快的常规流密码,这例如也可以允许更多处理器性能用于视频数据的处理而不是用于未压缩视频数据的内容保护操作。当用硬件实现时,获得相同的性能将需要更少的门。

[0036] 于此描述的技术不限于任何具体的硬件或软件配置;可以在任何计算或处理环境中找到它们的适用性。此技术可以用硬件、软件、或两者的组合来实现。此技术可以用运行在诸如移动或静止的计算机、个人数字助理、机顶盒、蜂窝电话和寻呼机、及其他电子设备之类的可编程机器上的程序来实现,所述电子设备均包括处理器、处理器可读存储介质(包括易失性和非易失性存储器和/或存储元件)、至少一个输入设备、以及一个或多个输出设备。程序代码被施加给利用输入设备输入的数据,以执行所述功能以及产生输出信息。输出信息可以被施加给一个或多个输出设备。本领域普通技术人员可以理解,本发明可以用各种计算机系统配置来实践,包括多处理器系统,小型计算机,大型计算机等。本发明还可以在分布式计算环境内实践,其中,任务可以由通过通信网络链接的远程处理设备来执行。

[0037] 每个程序可以用与处理系统相通信的高级程序或面向对象的编程语言来实现。然而,如果需要,程序可以用汇编或机器语言来实现。任何情况下,语言可以被编译或解释。

[0038] 程序指令可被用于使采用指令编程的通用或专用处理系统执行于此所述的操作。可替换地,所述操作可以由包含用于执行该操作的硬接线的逻辑电路的专用硬件元件、或由编程式计算机组件和常规硬件组件的任何组合来执行。于此描述的方法可以作为计算机程序产品来提供,计算机程序产品可以包括具有将指令存储于其上的机器可读介质,所述指令可被用于对处理系统或其他电子设备进行编程,以执行所述方法。于此所用的术语“机器可读介质”将包括任何能够存储或编码机器执行的指令序列并且能使机器执行于此描述的任一方法的介质。术语“机器可读介质”因此将包括但不限于固态的存储器、光和磁盘、以及将数据信号进行编码的载波。而且在本领域中,谈到软件以一种形式或其他形式(例如,程序、步骤、处理、应用、模块、逻辑等)采取动作或产生结果是很普遍的。这种表达仅仅是说明软件通过处理系统的运行而促使处理器执行产生结果的动作的简略方式。

[0039] 尽管已经参照说明性实施例说明了本发明,但并未意欲用限制的理解来解释本说明书。说明性实施例以及本发明其他实施例的各种修改,对与本发明相关的领域的技术人员而言是显而易见的,被认为处于本发明的精神和范围之内。

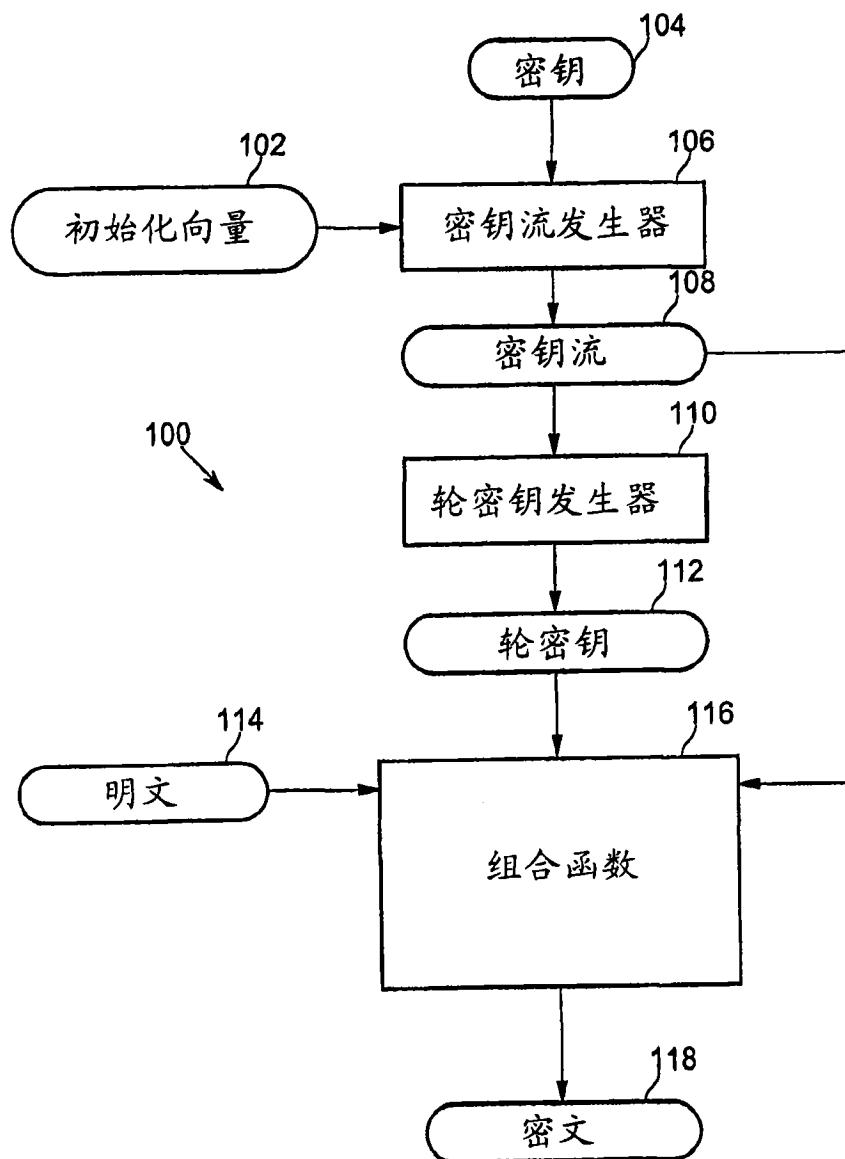


图 1

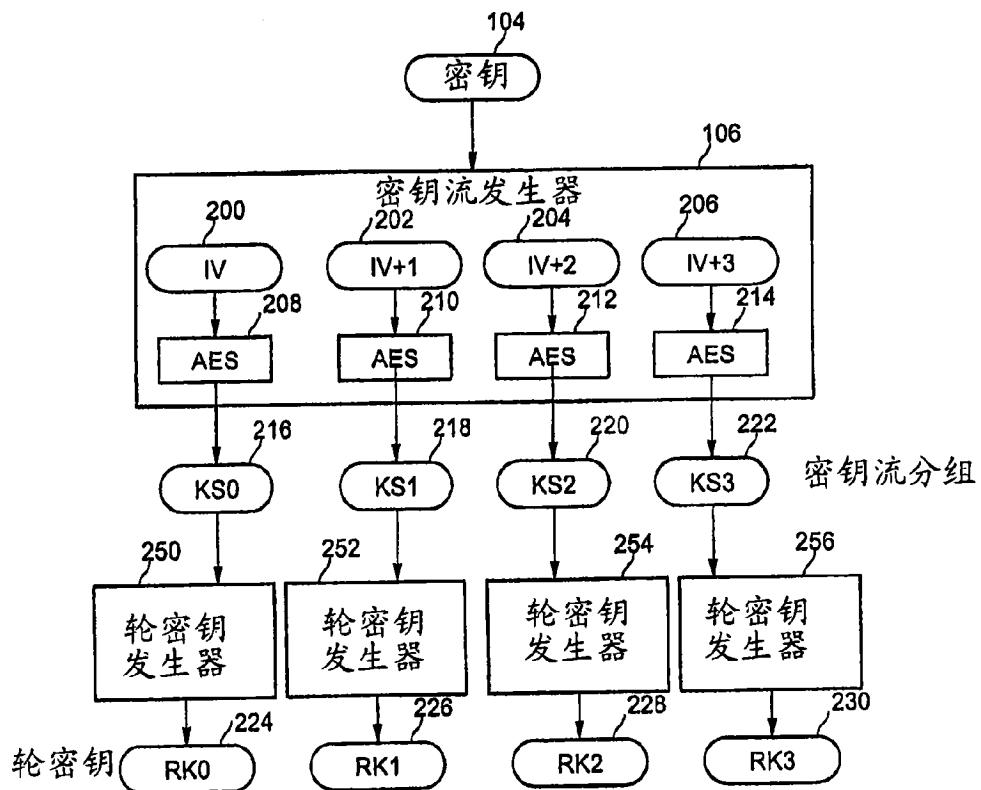


图 2

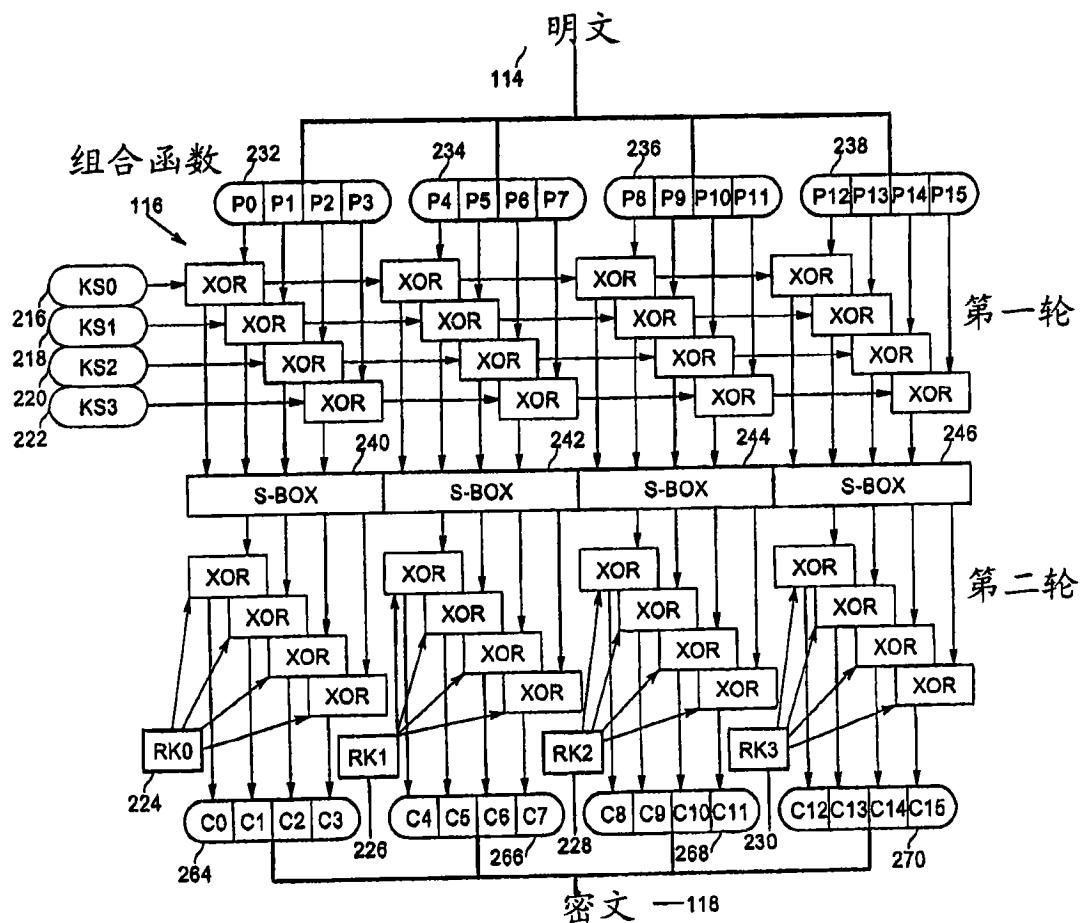


图 3

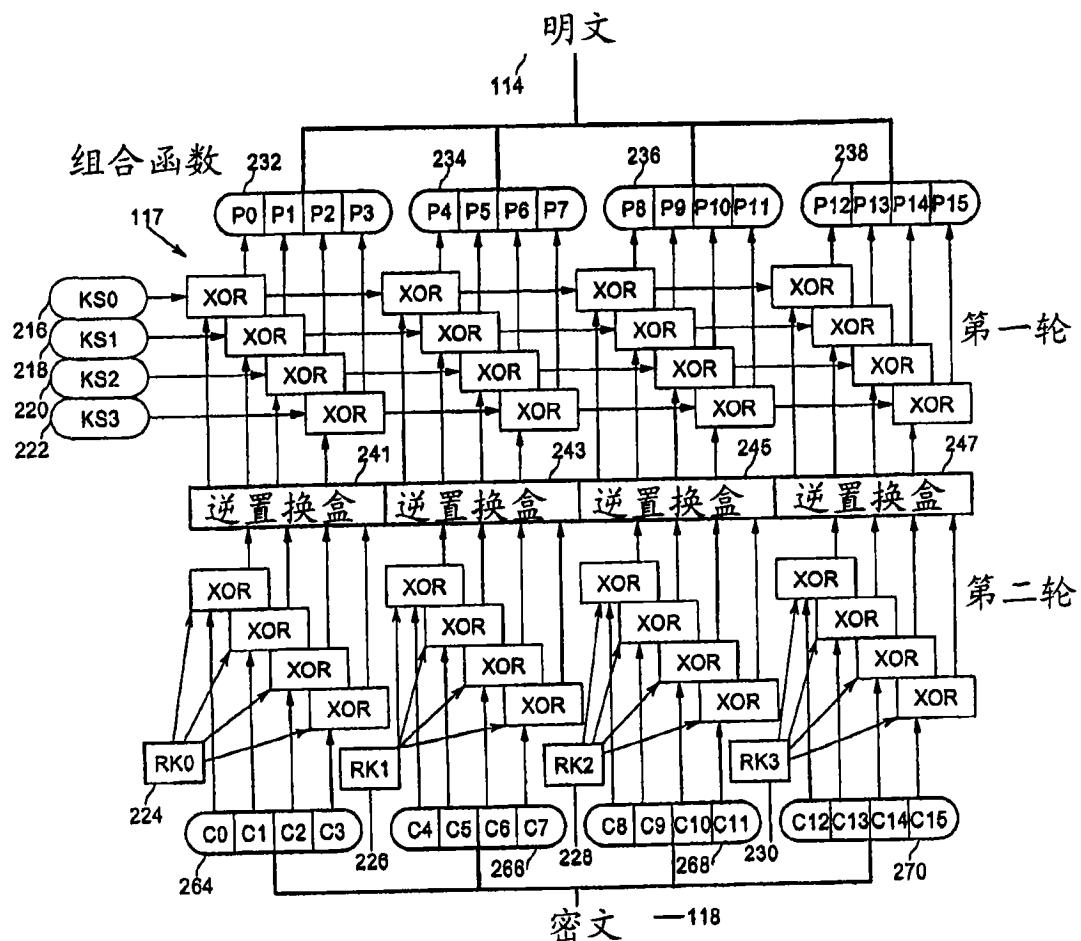


图 4