(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 1992589 B
(45)授权公告日 2011.09.07

(21)申请号 200610143977.4
(22)申请日 2006.11.08
(30)优先权数据
05110495.8 2005.11.08 EP
(73)专利权人 耶德托存取公司
地址 荷兰霍夫多普
(72)发明人 安东尼斯·J·P·M·范德文
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 马浩
(51)Int.Cl.
H04L 9/18(2006.01)
H04L 9/06(2006.01)
(56)对比文件
CN 1595978 A,2005.03.16,
CN 1244321 A,2000.02.09,
EP 0725511 A2,1996.08.07,
审查员 胡丽丽

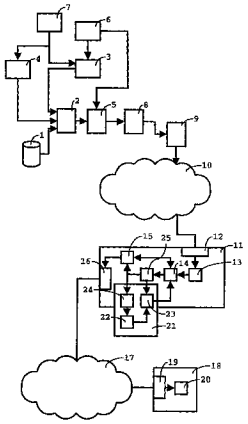
权利要求书 4 页 说明书 10 页 附图 5 页

(54)发明名称

加扰和解扰数据单元的方法

(57)摘要

一种加扰数据流的方法，包括从数据流中获取一串第一数据块(P_i)序列(29,30)，反转每个第一块(P_i)序列(29,30)中的块的顺序来形成相应的第二数据块序列(31,37)，以及在块链接模式中用一个密码(E_k)加密每个第二块序列(31,37)中的块，被每个第二块序列(31,37)的相应初始化矢量(IV_3,IV_N)所初始化，对于流中数据单元(26)所包括的一连串第一块序列(29,30)，生成至少一个初始化矢量(IV_N)用于加密所述单元中由第一块序列(30)所形成的第二块序列(37)，这依赖于所述单元中先前的第一块序列(29)中的至少一个块。



CN 1992589 B

1. 一种加扰数据流的方法，包括

从所述数据流中获取一串第一数据块序列，

反转每个第一数据块序列中的数据块 (Pi) 的顺序来形成相应的第二数据块序列，以及

在块链接模式中用一个密码 (E_k) 加密每个第二数据块序列中的块，该密码 (E_k) 被每个第二数据块序列的相应初始化矢量所初始化，

其中，

针对所述流中的数据单元 (26) 中所包括的所述一串第一数据块序列，用于加密由所述单元中的一个第一数据块序列所形成的第二数据块序列的至少一个初始化矢量是依赖于所述单元中的在前第一数据块序列中的至少一个块而生成的。

2. 如权利要求 1 所述的方法，其中用于加密由所述单元 (26) 中的第一数据块序列所生成的第二数据块序列的每个初始化矢量是依赖于所述单元 (26) 中任何在前第一数据块序列中每一个的至少一个块而生成的。

3. 如权利要求 1-2 中任何一个所述的方法，包括接收数据包 (27)，其中该数据包 (27) 包括报头 (28) 和有效载荷，其中所述单元由有效载荷组成。

4. 如权利要求 1-2 中任何一个所述的方法，其中密码 (E_k) 为一个块密码，被配置用来处理预定大小的基本块，其中至少第二数据块序列中的块 (P_i) 在大小上对应于所述基本块的大小。

5. 如权利要求 4 所述的方法，其中如果所述单元 (26) 由所述一串第一数据块序列和随后的在大小上少于基本块大小的倍数的数据量组成，

将所述数据量填充成等于基本块的大小的倍数的大小，以形成至少两个块的第一末尾块序列，

交换第一末尾块序列的最后两个块，并且反转第一末尾块序列的块的顺序以形成第二末尾数据块序列 (40)，

在块链接模式中使用密码 (E_k) 来加密第二末尾数据块序列 (40) 的块，该密码 (E_k) 依赖于所述单元的在前第一数据块序列中的至少一个块而生成的一个初始化矢量进行初始化。

6. 如权利要求 4 所述的方法，其中如果所述单元由一个或者更多个预定数目块的第一数据块序列和在大小上相当于少于一个基本块大小的数据量组成，

将该数据量填补成一个相当于基本块的大小的大小，来形成一个最后的块 (42)，

在块链接模式中使用密码 (E_k) 来加密最后的块 (42)，该密码 (E_k) 依赖于所述单元的任何在前第一数据块序列中的至少一个块而生成的第一初始化矢量进行初始化。

7. 如权利要求 6 所述的方法，其中所述第一初始化矢量是基于独立于所述单元中任何在前第一数据块序列的任何块的矢量，通过在所述至少一个初始化矢量上执行密码操作来产生的。

8. 如权利要求 7 所述的方法，其中所述密码操作是解密操作。

9. 一种加扰数据流的方法，包括

从所述数据流中获取一串第一数据块序列，

反转每个第一数据块序列中的数据块 (Pi) 的顺序来形成相应的第二数据块序列，以

及

在块链接模式中用一个密码 (E_k) 加密每个第二数据块序列中的块，该密码 (E_k) 被每个第二数据块序列的相应初始化矢量所初始化，

其中，

针对所述流中的数据单元 (26) 中所包括的所述一串第一数据块序列，用于加密由所述单元中的一个第一数据块序列所形成的第二数据块序列的至少一个初始化矢量是依赖于该同一第一数据块序列中最后一块之前的至少一个数据块而生成的。

10. 如权利要求 9 所述的方法，包括接收数据包 (27)，其中该数据包 (27) 包括报头 (28) 和有效载荷，其中所述单元由有效载荷组成。

11. 如权利要求 9 所述的方法，其中密码 (E_k) 为一个块密码，被配置用来处理预定大小的基本块，其中至少第二数据块序列中的块 (P_i) 在大小上对应于所述基本块的大小。

12. 如权利要求 11 所述的方法，其中如果所述单元 (26) 由所述一串第一数据块序列和随后的在大小上少于基本块大小的倍数的数据量组成，

将所述数据量填充成等于基本块的大小的倍数的大小，以形成至少两个块的第一末尾块序列，

交换第一末尾块序列的最后两个块，并且反转第一末尾块序列的块的顺序以形成第二末尾数据块序列 (40)，

在块链接模式中使用密码 (E_k) 来加密第二末尾数据块序列 (40) 的块，该密码 (E_k) 依赖于所述单元的在前第一数据块序列中的至少一个块而生成的一个初始化矢量进行初始化。

13. 如权利要求 11 所述的方法，其中如果所述单元由一个或者更多个预定数目块的第一数据块序列和在大小上相当于少于一个基本块大小的数据量组成，

将该数据量填补成一个相当于基本块的大小的大小，来形成一个最后的块 (42)，

在块链接模式中使用密码 (E_k) 来加密最后的块 (42)，该密码 (E_k) 依赖于所述单元的任何在前第一数据块序列中的至少一个块而生成的第一初始化矢量进行初始化。

14. 如权利要求 13 所述的方法，其中所述第一初始化矢量是基于独立于所述单元中任何在前第一数据块序列的任何块的矢量，通过在所述至少一个初始化矢量上执行密码操作来产生的。

15. 如权利要求 14 所述的方法，其中所述密码操作是解密操作。

16. 一种用于加扰数据流的系统，包括

一个输入端，用于接收所述数据流作为一串第一数据块序列，

多个寄存器以及至少一个逻辑单元，用于反转每个第一数据块序列中的数据块的顺序来形成相应的第二数据块序列，以及

一个处理装置，用于在块链接模式中用一个密码 (E_k) 加密每个第二数据块序列中的数据块，该密码 (E_k) 由每个第二数据块序列相应的初始化矢量进行初始化，

其中，

该系统被配置为：针对包括在所述流中的数据单元 (26) 中的所述一串第一数据块序列，用于加密由所述单元中的一个第一数据块序列所形成的第二数据块序列的至少一个初始化矢量依赖于所述单元 (26) 中的在前第一数据块序列中的至少一个块而生成。

17. 一种解扰加扰的数据流来形成数据流的方法，包括

从所述加扰数据流中获取一串加扰数据块序列，以及

通过在反转链接模式中使用一解密密码 (D_k) 来解扰每个加扰数据块序列以形成一个相关的解扰数据块序列，其中，解扰加扰数据块序列，

通过向相关的加扰数据块序列中的最后一个块应用所述解密密码 (D_k)、以及应用至少以应用解密密码 (D_k) 的结果和一初始化矢量作为操作数的算符，来获得解扰数据块序列中的最后一个块，并且其中通过对加扰数据块序列上相应位置的块应用所述解密密码 (D_k)、以及应用至少以应用解密密码 (D_k) 的结果和在加扰数据块序列中在所述相应位置之前的下一位置的加扰数据块作为操作数的算符，来获得在解扰数据块序列中最后块之前的每个块，

其中，

针对包括在加扰数据流中数据单元中的一串加扰数据块序列，用于解扰所述单元中的一个加扰数据块序列的至少一个初始化矢量，是依赖于通过解扰所述单元中的在前加扰数据块序列而获得的解扰数据块序列中的至少一个解扰数据块而生成的。

18. 如权利要求 17 所述的方法，其中，用于解扰每个加扰数据块 (C_i) 序列的相应初始化矢量是依赖于通过对在相同加扰数据块序列中最后的加扰数据块之前的加扰数据块序列中的一个块应用所述解密密码 (D_k)、以及通过应用至少以应用解密密码的结果和相同加扰数据块序列中的所述一个块之前的下一位置的加扰数据块作为操作数的算符而获得的至少一个数据块，而生成的。

19. 如权利要求 17 所述的方法，其中用于解扰所述单元中的各加扰数据块序列的每个初始化矢量的生成，依赖于来自由解扰所述单元中的在前加扰数据块序列而得到的任何解扰数据块序列中每一个的至少一个解扰数据块。

20. 如权利要求 17-19 中任何一个所述的方法，包括接收数据包 (34)，所述数据包 (34) 包括报头 (35) 和有效载荷，其中所述单元由有效载荷组成。

21. 如权利要求 17-19 中任何一个所述的方法，其中所述解密密码 (D_k) 为一个块密码，该块密码被配置为处理预定大小的基本块，其中各加扰数据块序列中的块 (C_i) 在大小上对应于所述基本块的大小。

22. 如权利要求 21 所述的方法，其中，如果单元由一串加扰数据块序列以及随后的在大小上等于基本块大小的整数倍和基本块大小的一部分 (C_N) 的数据量组成，

将该数据量用预定的数据填补成等于基本块的大小的倍数的大小，来形成一个加扰数据块末尾序列；

形成一解扰数据块末尾序列的最后一个块 (P_N)，这是通过对紧接在加扰数据块末尾序列中的最后的块之前的一个块应用解密密码、应用以应用解密密码的结果和加扰数据块末尾序列的所述最后块作为操作数的异或算符、以及删除对应所述预定数据大小的作为所述异或算符结果的部分 (C') 来实现的；

形成解扰数据块末尾序列中最后两个块 (P_{N-1}, P_N) 之前的任何一个块，这是通过向加扰数据块末尾序列中相应位置的一个块应用解密密码 (D_k)、以及应用以应用解密密码的结果和加扰数据块末尾序列中在所述相应位置之前的下一位置的一个加扰数据块作为操作数的异或算符来实现的；以及

获得解扰数据块末尾序列中最后块 (P_N) 之前的一个块 (P_{N-1})，这是通过将所述对应所述预定数据大小的所删掉的部分 (C') 和加扰数据块末尾序列的最后块进行串连而形成的一个块 (52) 应用解密密码、以及应用以应用解密密码的结果和依赖于由解扰所述单元中一个在前加扰数据块序列而得到的任何解扰数据块序列中至少一个的至少一个块所产生的初始化矢量作为操作数的异或算符来实现的。

23. 如权利要求 21 所述的方法，其中，如果下一个单元由零或者更多个预定数目块的加扰数据块序列和在大小上少于一个基本块大小的随后数据量 (C_N) 组成，

那么将该数据量填补成一个基本块的大小，以形成一个最后的块 (53)，

在块链接模式中使用解密密码 (D_k) 来解密最后的块 (53)，该解密密码 (D_k) 由第一初始化矢量进行初始化，该第一初始化矢量的生成依赖于由解扰所述单元中的在前加扰数据块序列获得的任何解扰数据块序列中至少一个的至少一个块。

24. 如权利要求 23 所述的方法，其中基于独立于由解扰所述单元中的在前加扰数据块序列而获得的任何在前解扰数据块中的任何块的至少一个矢量在所述至少一个初始化矢量上执行密码操作，来生成所述第一初始化矢量。

25. 如权利要求 24 所述的方法，其中所述密码操作是应用所述解密密码进行解密。

26. 一种用于解扰加扰数据流以形成数据流的系统，包括

一个输入端，用于接收所述加扰数据流，作为一串加扰数据块序列，以及

一个处理装置，用于解扰每个加扰数据块序列以形成一个相关的解扰数据块序列，这是通过使用用于解扰加扰数据块序列的反转链接模式中的解密密码 (D_k) 来实现的，

获得所述解扰数据块序列中的最后一个解扰数据块，这是通过向相关的加扰数据块序列中的最后一个块应用解密密码 (D_k)、以及应用至少以应用解密密码 (D_k) 的结果和一初始化矢量作为操作数的算符来实现的，并且获得所述解扰数据块序列中的每个在前的解扰数据块，这是通过对加扰数据块序列上相应位置的块应用解密密码、以及应用至少以应用解密密码的结果和在加扰数据块序列中在所述相应位置之前的下一位置的加扰数据块作为操作数的算符来实现的，

其中，

该系统被配置为：针对包括在所述加扰数据流中的数据单元内的一串加扰数据块序列，用于解扰所述单元中的一个加扰数据块序列的至少一个初始化矢量依赖于通过解扰所述单元中的在前加扰数据块序列而获得的解扰数据块序列中的至少一个解扰数据块而生成。

加扰和解扰数据单元的方法

技术领域

[0001] 本发明涉及一种加扰数据流的方法，包括

[0002] 从数据流中获取一串第一数据块序列，

[0003] 反转每个第一块序列中的块的顺序来形成相应的第二数据块序列，以及

[0004] 在块链接模式中用一个密码加密每个第二块序列中的块，被每个第二块序列的相应初始化矢量所初始化。

[0005] 本发明也涉及一种用于加扰数据流的系统，包括

[0006] 一个输入端，用于接收作为一串第一数据块序列的流，

[0007] 多个寄存器以及至少一个逻辑单元，用于反转每个第一块序列中的块的顺序来形成相应的第二数据块序列，以及

[0008] 一个处理装置，用于在块链接模式中用一个密码加密每个第二块序列中的块，由每个第二块序列相应的初始化矢量进行的初始化。

[0009] 本发明也涉及一种解扰被加扰的数据来形成数据流的方法，包括

[0010] 从加扰数据流中获取一串加扰数据块的序列，以及

[0011] 通过使用在反转链接模式中的一解密密码来解扰每个加扰的数据块序列以形成一个相关的解扰数据块的序列，其中，解扰一加扰数据块序列，

[0012] 通过向所述相关加扰数据块序列中的最后一个块应用所述解密密码、以及应用以至少一初始化矢量和所述解密密码的结果作为操作数的算符，来获得所述解扰数据块序列中的最后一个块，并且其中通过对加扰数据块序列上相应位置的块应用所述解密密码、以及应用以至少所述解密密码的结果和在加扰数据块序列中下一位置的加扰数据块作为操作数的算符，来获得在解扰数据块序列中最后块之前的每个块。

[0013] 本发明也涉及一种解扰加扰的数据来形成数据流的系统，包括

[0014] 一个输入端，用于接收加扰数据流作为一串加扰数据块序列，以及

[0015] 一个处理装置，用于解扰每个加扰的数据块序列以形成一个相关的解扰数据块的序列，这是通过使用反转链接模式中的解密密码来实现，其中，解扰加扰的数据块序列，

[0016] 获得解扰数据块序列中的最后一个块，这是通过向相关加扰数据块序列中的最后一个块应用所述解密密码、以及应用以至少一初始化矢量和所述解密密码的结果作为操作数的算符，以及获得在解扰数据块序列中最后块之前的每个块，这是通过对加扰数据块序列上相应位置的块应用所述解密密码、以及应用以至少所述解密密码的结果和在加扰数据块序列中下一位置的解扰数据块作为操作数的算符。

[0017] 本发明也涉及一种用于发送和接收数据的设备。

[0018] 本发明还涉及一种计算机程序。

[0019] 这些方法和系统的相应实施例可以从 WO95/10906 中得知。在所述已知的方法中，数字数据被分成 N 块的包，X(1)，X(2)，……X(N)，其中每个块具有 2^m 个比特。块序列在加密操作进行前被翻转成 X(N)，X(N-1)，……X(1)。这个块序列用加密算法 E 以如下方法进行加密（其中 ^ 用来表示异或 (XOR) 算符）：

[0020] Y(1) = E[X(N)^IV]

[0021] Y(i) = E[X(N-i+1)^Y(i-1)] 其中 i > 1 且 i ≤ N。

[0022] 再次将这些加密的块进行反转，从而将序列 Y(N)，Y(N-1)，……Y(1) 传输到接收器。

[0023] 在接收器端，解密算法 D 的装置这样获得原始数据块：

[0024] X(i) = D[Y(N-i+1)^Y(N-i)] 其中 i = 1,2，……，N-1

[0025] X(N) = D[Y(1)]^IV

[0026] 所述已知系统中所使用的方法被称为反转密码块链接或者说 RCBC 方法。这显示出了接收器的缓冲存储器仅需要存储两个数据块的优点。

[0027] 已知方法和系统的问题在于，它要求在发送器端缓冲器具有存储 N 个块的容量，以便实现块序列的反转。这在具有许多加密数据发送器的数据通信系统、或者同时具有数据发送器和接收器功能的设备中成为了一个问题。

发明内容

[0028] 本发明的一个目的在于提供一种类型的方法、系统、设备和计算机程序，用于在提供可接受的内容保护等级的同时可以更加高效地打开段。

[0029] 该目的通过根据本发明的加扰数据流的方法实现，其特征在于，针对流中数据单元所包括的一连串第一块序列，依赖于所述单元中先前的第一块序列中的至少一个块，生成至少一个初始化矢量用于加密单元中由第一块序列所形成的第二块序列。

[0030] 由于数据单元包括一串第一块序列，每个第一块序列由较少的块形成，这意味着反转块的顺序需要较少的缓冲存储。这有可能得到满意的安全等级，因为至少两个第二块序列被有效地链接了。这个链接是由于如下事实，根据所述单元中先前第一块序列中的至少一个块，生成至少一个初始化矢量——在要求最高安全性的情况下是除了第一个之外的每一个——用于加密从第一块序列形成的第二块序列。

[0031] 在一个实施例中，依赖于相同第一序列中最后一块之前的至少一个数据块，生成相应的初始化矢量，以用于加密由第一块序列所形成的每个第二块序列中的块。

[0032] 这样的效果是实现了初始化矢量中更多的变化。即使一个单元中包括的串中第一块序列的第一个的块都用一个很大可能是唯一的初始化矢量进行加扰。变化的保证是通过依赖于相同第一序列最后一块之前的至少一个数据块生成所述初始化矢量而实现的。由于每个第一序列中块的顺序的反转，在解密器要求初始化矢量之前，生成所述初始化矢量所依赖的一个或多个数据块就可以在解密过程中获得。因此，可能以相对高的可能性来实现所述单元中包括的一串第一序列中每个第一序列的初始化矢量的唯一性，而不需要向接收器为每个第一序列的提供一个新的初始化矢量。

[0033] 在一个实施例中，依赖于所述单元中任何先前的第一块序列中每一个的至少一个块，来生成每个初始化矢量，以用于加密由所述单元中第一块序列所生成的第二块序列。

[0034] 因此，第二序列之间的链接是最大的，因为在没有预先获得单元中第一序列串中的所有先前第一块序列的情况下，最后一个第一数据块序列不能不用密码 (in the clear) 得出。

[0035] 一个实施例包括接收数据包，其中该数据包包括报头和有效载荷，所述单元由有

效载荷组成。

[0036] 这是更优的实施例，因为有效载荷可以被加扰而不需要首先对其全部缓冲。

[0037] 在一个实施例中，所述密码为一个块密码，被配置用来处理预定大小的基本块，其中至少第二数据序列中的块在大小上对应于所述基本块大小。

[0038] 在一个实施例中，如果所述单元由第一块序列的串和随后的在大小上相当于少于所述基本块大小的倍数的数据量组成，

[0039] 将所述数据量填充到等于基本块的大小的倍数的大小，以形成至少两个块的第一末尾序列，

[0040] 交换第一末尾块序列的最后两个块，并且反转第一末尾块序列的块的顺序以形成第二末尾数据块序列，

[0041] 使用在块链接模式中的密码来加密第二末尾数据块序列的块，由依赖于所述单元的先前第一块序列中至少一个块所生成的初始化矢量来进行初始化。

[0042] 因此，该方法适于实现某种形式的密文挪用 (ciphertextstealing)。这是保证整个单元都被加扰的一种相关安全方法。此外，它允许使用由预定数目的块组成的第一序列来加扰所述单元的第一部分。

[0043] 在一个实施例中，如果流中的下一个单元由零或者更多个预定数目块的第一序列和在大小上相当于少于一个基本块大小的数据量组成，

[0044] 那么将该数据量填补成一个相当于基本块的大小，来形成一个最后的块。

[0045] 使用块链接模式中的密码来加密最后的块，被依赖于所述单元的一个先前第一块序列中的至少一个块所生成的初始化矢量进行初始化。

[0046] 因此，随后的数据量不需要不用密文 (in the clear) 地传输，即使其数据量少于所述密码配置的所述基本块大小。

[0047] 在本实施例的一个变体中，初始化矢量是通过在一个矢量上执行密码操作（优选地是一个解密，是所述密码的反转）来产生，基于独立于单元中任何先前第一块序列的任何块的至少一个矢量。

[0048] 其效果在于所述初始化矢量的变化可以通过使用与用来生成加扰先前单元的块数据的一个初始化矢量的相同矢量来实现。因此，需要传输给解扰器的矢量更少，同时保持了一样好的安全性。使用作为所述密码的反转的解密，效果在于使用了为了解码目的已经存在的的解扰器的硬件和 / 或软件配置。

[0049] 根据另一方面，本发明的加扰数据流的系统，其特征在于，针对包括在流中数据单元中的一串第一块序列，系统被配置为依赖于所述单元中先前的第一块序列中的至少一个块，生成至少一个初始化矢量，用于加密由单元中第一块序列所形成的第二块序列。

[0050] 出于对效率的考虑，该系统非常适于包含在专用加密处理器中。

[0051] 优选地，系统被配置来执行根据本发明的一种方法。

[0052] 根据另一方面，本发明的解扰被加扰数据流的方法，其特征在于，针对包括在加扰数据流中数据单元内的一串加扰数据块序列，依赖于通过解扰所述单元中一个先前加扰数据块序列而获得的解扰数据块序列中的至少一个解扰数据块，生成至少一个初始化矢量用于解扰被加扰的数据块序列。

[0053] 该方法适合解扰那些使用根据本发明的加扰数据流的方法所获得的加扰数据。由

于串中的数据块序列是分离的、并且按次序解扰的，所以如果序列中的块不是按次序（例如，反转次序）接收的也没有关系，因为序列比整个序列串要短。由于依赖于通过解扰所述单元中一个先前加扰数据块序列而获得的解扰数据块序列中的至少一个解扰数据块，来生成至少一个初始化矢量用于解扰被加扰数据块序列，至少两个加扰数据的块序列是链接的，使得非法解扰变得更加困难。

[0054] 在一个实施例中，依赖于通过对在相同序列中最后的加扰数据块之前的加扰数据块序列中的块应用所述解密密码、以及通过应用以至少在相同加扰数据块序列的下一位置的加扰数据块和所述解密密码的结果作为操作数的算符而获得的至少一个数据块，来生成相应初始化矢量用于解扰每个加扰数据块序列。

[0055] 这样的优点是，多个单元的流不需要为了实现初始化矢量的有效变化，而将大量初始化矢量从加扰器传输到解扰器。

[0056] 在一个实施例中，每个用于解扰所述单元中的加扰数据块序列的初始化矢量的生成，依赖于来自解扰所述单元中一个先前的加扰数据块序列而得到的任何解扰数据块序列中每一个的至少一个解扰数据块。

[0057] 因此，实际上，所述单元中包括的串中所有的序列都被链接了。

[0058] 一个实施例包括接收数据包，数据包括报头和有效载荷，其中单元由有效载荷组成。

[0059] 在一个实施例中，解密密码为一个块密码，其被配置为处理预定大小的基本块，其中加扰数据块序列中的块在大小上对应于所述基本块大小。

[0060] 在一个实施例中，如果所述单元由加扰数据块序列串以及随后的在大小上等于所述基本块大小的整数倍和所述基本块大小的一部分的数据量组成，

[0061] 将该数据量用预定的数据填补成等于基本块的大小的倍数，来形成一个加扰数据块的末尾序列，

[0062] 形成一解扰数据块末尾序列的最后一个块，这是通过对直接在加扰数据末尾序列最后的块之前紧邻的一个块应用所述解密密码、应用以解密密码的结果和所述末尾加扰数据块序列的最后块作为操作数的异或算符，以及删除对应预定数据大小的、作为异或算符结果的一部分，

[0063] 形成解扰数据块末尾序列中最后两个块之前的任意一个块，这是通过向第一末尾加扰数据块序列中相应位置的一个块应用所述解密密码、以及应用具有解密密码的结果和末尾加扰数据块序列中下一位置的一个解扰数据块作为操作数的异或算符，以及

[0064] 获得解扰数据块末尾序列中最后块之前的一个块，这是通过对将对应预定数据大小的所删掉的部分和末尾加扰数据块序列的最后块进行串连而形成的块应用解密密码、以及应用以解密密码的结果和一个依赖于由解扰所述单元中一个先前加扰数据块序列所获得的至少一个解扰数据块而产生的初始化矢量为操作数的异或算符。

[0065] 这是一个在解扰器端的密文挪用（ciphertext stealing）的实施例。

[0066] 在一个实施例中，如果下一个单元由零或者更多个预定数目块序列和在大小上少于一个基本块大小的随后数据量组成，

[0067] 那么将该数量的数据填补成一个基本块的大小，以形成一个最后的块，

[0068] 使用块链接模式中的密码来加密最后的块，由初始化矢量进行初始化，该初始化

矢量的生成依赖于由解扰所述单元中一个先前的加扰数据块序列获得的任何解扰数据块序列中至少之一的至少一个块。

[0069] 使用预定块数目的序列的效果在于，不需要将每个序列中的块数目发送到解扰器。单元间的分界也是预定的，例如在单元由有效载荷的包组成的情况下，任何大小上小于密码的基本块大小的数据仍然可以加密的形式被发送到解扰器。与未加扰单元相比，不需要增加加扰单元的大小。

[0070] 在一个变体中，通过在一个矢量上执行密码处理（优选的，所述解密密码）来生成所述初始化矢量，这是基于至少一个矢量，该矢量独立于由解扰所述单元中先前加扰数据块序列而获得的任何先前解扰数据块中的任何块。

[0071] 这意味着解扰器不需要接收和存储多个用来导出初始化矢量的矢量。用来导出初始化矢量的矢量可以在流中一定数目的数据单元上保持不变。密码操作保证了决不将其直接作为操作数用于逻辑算符，例如异或算符。

[0072] 根据另一方面，根据本发明的用于解扰加扰数据流来形成数据流的系统，其特征在于，对于包括在加扰数据流中数据单元内的一串加扰数据块序列，依赖于通过解扰所述单元中一个先前加扰数据块序列而获得的解扰数据块序列中的至少一个解扰数据块，系统被配置为生成至少一个初始化矢量，用于解扰加扰的数据块序列。

[0073] 优选地，该系统配置用于执行根据本发明的一种解扰方法。

[0074] 根据本发明的另一方面，它提供了一种用于发送和接收数据的装置，包括配置为应用根据本发明的加扰数据流的方法以及根据本发明的解扰加扰数据流的方法的设备。

[0075] 因为互补的加扰和解扰的方法可以用同样的缓冲要求来实现，该装置不需要用于存储两个操作之一中所不使用的块的寄存器。因此，更经济地硬件实现变为可能，特别适用于一个被配置为同时具有发送器和接收器功能的设备，例如两个网络之间的网关。

[0076] 根据本发明的另一个方面，提供了包括一组指令的计算机程序，当同机器可读介质结合时，可以使一个系统具有信息处理能力，以执行根据本发明的加扰数据流的方法或根据本发明的解扰加扰的数据流的方法。

附图说明

[0077] 接下来参考附图对本发明进行更加详细的阐述，其中

[0078] 图 1 描述了用于实现加扰和解扰广播数据流方法的系统，

[0079] 图 2 描述了加扰数据流的方法的一个实施例，

[0080] 图 3 描述了在加扰数据流的方法中的密文挪用方法的一个实施例，

[0081] 图 4 描述了怎样处理组成 MPEG-2 传输流包的有效载荷末尾的单个部分块，

[0082] 图 5 描述了解扰数据流的方法的一个实施例，

[0083] 图 6 描述了在解扰器中密文挪用方法的一个实施例，

[0084] 图 7 描述了在解扰器中，怎样处理组成 MPEG-2 传输流包的有效载荷末尾的单个部分块。

具体实施方式

[0085] 图 1 描述了对广播数据应用加扰方法。所描述的系统的至少一部分使用的技术

基本可得知于“数字视频广播(DVB);ImplementingGuidelines of the DVB Simulcrypt Standard”,ETSI 技术报告 TR102035 v1.1.1,欧洲电信标准协会,2002。

[0086] 内容提供器 1 向复用单元 2 提供包流,包携带纯文本的、即未加扰的内容数据。授权控制信息(ECM)发生器 3 向复用单元 2 提供携带 ECM 的包流。授权管理信息(EMM)发生器 4 向复用单元 2 提供携带 EMM 的包流。这些流被复用成 MPEG-2 传输流(TS)包的单一流,并被提供给加扰器 5。MPEG-2 TS 包的语法在国际标准 ISO/IEC13818-1 中有更全面的描述。加扰器 5 执行加扰 MPEG-2 TS 包的有效载荷的方法将会在下面更详细地进行描述。它从 CW 发生器 6 接收控制字(CW),其用作一个块密码的密钥。

[0087] CW 发生器 6 向 ECW 发生器 3 提供 CW,ECW 发生器 3 用由用户授权系统(SAS)7 获得的一个会话密码将它们加密。SAS 提供带有对独立用户授权的会话密钥到 EMM 发生器 4。EMM 发生器包括这些密钥以及授权信息在 EMM 中,寻址到提供给单独用户的安全令牌。该安全令牌可包括软件代理,其使用例如用于避免软件中例程分析的代码模糊这样的特征来实现。安全令牌的其它例子包括,包含了处理器的设备,所述处理器被提供保护性特征以防止访问存储在其上的数据和/或布线其中的例程分析。

[0088] 将加扰数据流从加扰器 5 中传送到调制器 8,并从那里传送到发射器 9。发射器 9 在广播网络 10 上,例如卫星、电缆或地面网络、或包括多个这些网络的网络上,广播加扰数据流。在一个可替换的实施例中,加扰的 MPEG-2 TS 包流被进一步封装成数据包,并且在数据网络上广播、多播或单播,例如互联网协议上的网络。

[0089] 为了示意的目的,在图 1 中示出一个基本集成接收解码器(IRD)11。基本 IRD 包括用于接收经广播网络 10 发送的数据的网络适配器。解调器 13 使得加扰器/解扰器 14 可以获得加扰数据流。所述加扰器/解扰器 14 被配置为用于同时执行解扰数据流的方法和加扰数据流的方法。处理器 15 控制基本 IRD 11 的操作。它可以将由加扰器/解扰器 14 产生的加扰数据流引导到第二网络适配器 16 中,其将基本 IRD11 连接到本地网络 17 上。本地网络 17 可以是一个家庭网络,例如基于 IEEE 1394 标准。所提供的第二接收器 18 具有相应的网络适配器 19 和解扰器芯片 20。进一步的部件没有详细示出。解扰器芯片 20 执行与加扰器/解扰器 14 相同的方法。因为这个原因,将不再进一步进行描述。

[0090] 回到加扰器/解扰器 14,这个部件将使用条件访问子系统(CASS)21 提供的 CW 来解扰加扰的 MPEG-2 TS 包。CASS 21 与一安全处理设备 22 相连,例如将用于解密 CEM 的密钥提供给第一解密器 23 的智能卡。第一解密器 23 获得传送到加扰器/解扰器 14 的 CW。第二解密器 24 解密 EMM,来向安全处理设备 22 提供用于获取服务密钥所需的信息。处理器指导去复用单元 25 来重新获得携带 ECM 和 EMM 的 MPEG-2 TS 包,从而将它们提供给 CASS 21。

[0091] 图 2 描述了加扰数据流的方法的实施例,例如由加扰器 5 和/或加扰器/解扰器 14 来完成。在所描述的实施例中,该方法是在由 MPEG-2 TS 包 27 的有效载荷 26 组成的数据单元上实现的,MPEG-2TS 包 27 进一步包括报头 28。报头 28 不被加扰,而是不用密文地保留。显然该方法可以在其他类型的包上实现,而并不需要用一个传输层网络协议来定义。例如,该方法也可以在 MPEG-2 TS 包 27 中携载的节目元素流(PES)包上实现。

[0092] 尽管 MPEG-2 TS 包 27 具有固定长度,188 字节,有效载荷 26 不是这样。这是由于改变了包头 28 的长度。在图 2 描述的实施例中,有效载荷 26 的大小,可以被划分成固定大

小的基本块 P_i 的整数倍，也等同于所谓的超级块的整数倍。每个超级块是由一个基本块 P_i 的第一序列组成。第一个第一序列 29 和最后一个第一序列 30 被明确地示出。一串超级块构成了有效载荷 26。在一个实施例中，每个超级块由三个基本块 P_i 的第一序列 29，30 组成。在另一个实施例中，每个超级块可能有两个基本块 P_i。每个超级块中也可以有多于三个，例如，四个、五个或十个基本块。更多的数量要求加扰器 5 和 / 或加扰器 / 解扰器 14 中有更多的寄存器。

[0093] 下面进一步讨论当有效载荷 26 的大小不等于由整数个基本块 P_i 组成的超级块的整数倍的情况下，所进行的步骤。

[0094] 在本方法的另一个变化（未示出）中，有效载荷 26 被分成可变大小的超级块，即包含可变数目的基本块 P_i。

[0095] 基本块的大小优选地由块密码 E_k 来确定，一个对称的密钥密码，其伴随不变的转换作用于固定长度的比特组（基本块）。在所描述的实施例中，块密码 E_k 用于在 CW 下加密单独的基本块 P_i。合适的密码例子包括 DES，三重 DES 以及 AES/Rijndeal。因此，基本块的大小通常是 128 比特。

[0096] 在本发明的第一个步骤中，反转第一个第一序列 29 中基本块 P_1-P_3 来形成第一个第二序列 31。

[0097] 在第二个步骤中，在密码块链接模式中使用块密码 E_k 来加密第一个第二序列 31 中的三个基本块 P_1-P_3，其由与第一个第二序列相关的初始化矢量 IV_3 进行初始化。用于查找初始化矢量 IV_3 的、与基本块的第一个第二序列 31 相关的索引，就是序列中最后的基本块 P_3 的索引，这将贯穿本文所述的情况。用于加密基本块的相关第一个第二序列 31 的初始化矢量 IV_3 是应用异或算符所形成的，其操作数为长期固定的初始化矢量 IV_0 和在基本块 P_1-P_3 的第一个第一序列 29 最后一个基本块 P_3 之前的两个基本块 P_1，P_2 之间的异或。

[0098] 加扰有效载荷 26 的方法被配置成，长期固定的初始化矢量 IV_0 从不直接被用作初始化矢量。它从不直接用在第二（即反转的）块序列中的第一基本块 P_i 的块密码 E_k 操作之前紧邻的异或操作。由于这个原因，它可以用于多个 MPEG-2 TS 包 27，而基本上不会使破译变得更加简单。长期固定的初始化矢量 IV_0 不需要保密。当这里概述的加扰和解扰数据单元的方法用于点对点通信时，它就是已知的。在图 1 所示的情况下，其中单个的提供器控制发送器和接收器，对长期固定的初始化矢量 IV_0 可以进行保密。例如，它可以在 ECM 或 EMM 中提供。在一个可替换的实施例中，通过对报头 28 中包括的数据应用预定的算法，来获得独立于要加扰的数据的一个矢量，用于从中导出初始化矢量。

[0099] 因为用于加密块的相关第一个第二序列 31 中的块 P_1-P_3 的初始化矢量 IV_3，依赖于作为其获得来源的第一个第一序列 29 中最后块 P_3 之前的至少一个数据块而生成，所以实现了初始化矢量的更多变化。

[0100] 加密第一个第二序列 31 的结果是加扰块 C_3-C_1 的第一个第一序列 32。在所描述的实施例中，加扰块 C_3-C_1 的顺序被反转来形成加扰块 C_1-C_3 的第一个第二序列 33。将加扰块 C_1-C_3 的第一个第二序列 33 插入到加扰的 MPEG-2 TS 包 34 中，其包括一个未加密的报头 35 和一个加扰的有效载荷 36。

[0101] 因此，对于基本块 P_i，$i = 1...M$ 的第一个第一序列 29 来说，加密的基本块 C_i 按照如下方法获得：

[0102] $C_M = E_k[P_M \hat{} IV_M]$

[0103] $C_i = E_k[P_i \hat{} C_{i+1}]$，i = M-1...1。

[0104] 通常，加密的基本块按如下方式建立：

[0105] $C_{j.M} = E_k[P_{j.M} \hat{} IV_{j.M}]$

[0106] $C_{(j-1).M+i} = E_k[P_{(j-1).M+i} \hat{} C_{(j-1).M+i}]$，i = M-1...1，j = 1...N\M。

[0107] 符号“\”指的是商或者比值的整数部分。

[0108] 在所描述的实施例中，用于加密第 j 个第二序列中的块的初始化矢量 $IV_{j.M}$ 按照如下方法获得：

[0109] $IV_{j.M} = IV_0 \hat{} P_1 \hat{} ... P_i \hat{} P_{j.M-1}$。

[0110] 因此，用于加密通过反转块顺序且由第一块序列所形成的每个第二块序列中的块的各个初始化矢量，依赖于在相同第一序列中最后一块之前的至少一个数据块而生成。在该实施例中，它们的生成依赖于在相同第一序列中最后一块之前的所有数据块。

[0111] 不仅如此，用于加密由包有效载荷 26 中的第一块序列形成的第二块序列的每个初始化矢量是依赖于至少一个块产生的，在这种情况下是所有块，在基本块或“超级块”的任何先前第一序列的每一个中。

[0112] 为了加密由反转最后的基本块第一序列 30 中的基本块顺序所得到的最后一个第二序列 37 中的块 P_{N-2}-P_N，再次在密码块链接模式中处理加密密码 E_k。通过执行长期固定的初始化矢量 IV_0 与最后一个基本块 P_N 之前每个基本块的异或运算，生成一个与最后一个第二基本块序列相关的初始化矢量 IV_N。其结果是加扰数据块的最后一个第一序列 38。反转块的顺序来获得加扰数据块的最后一个第二序列 39。

[0113] 图 3 描述了如果 MPEG-2 TS 包有效负载 26 由 N\M 整数个第一基本块序列以及随后在大小上少于 M 个基本块的数据量组成，那么如何进行加扰方法。在所描述的实施例中，最后的数据量可以被分成两个完整的基本块 P_{N-2}，P_{N-1} 以及一个部分块 P_N。最后的块 P_N 用零填充到与完整基本块相同的大小。因此，第一末尾序列由块 P_{N-2}，P_{N-1} 和所填充的第 N 个块 P_N 组成。交换第一末尾块序列的最后两个块的位置来形成第二末尾块序列 40（如图 3 所示）。用块链接模式中的加密密码 E_k 来加密第二末尾块序列 40 中的块。由于通过执行长期固定的初始化矢量 IV_0 与 MPEG-2 TS 包有效负载 26 中部分块 P_N 之前的最后一个完整基本块 P_{N-1} 之前每个基本块的异或运算，生成一个初始化矢量作为初始化矢量 IV_N。其结果是加扰数据块的第一末尾序列 41。从第一末尾块序列 41 的第一个块中，去除在大小和位置上对应于经填充增加的数据的一定量的加扰数据 C’，并接着反转块的顺序来获得一个第二末尾加扰块序列（未示出），将其插入到加扰的有效载荷 36 中。当然，可以在反转块的顺序之后将加扰数据 C’ 删除。

[0114] 如果 MPEG-2 TS 包有效负载 26 由 N\M 整数个第一基本块序列以及随后在大小上少于一个基本块的数据量组成，那么就采取图 4 中描述的操作。部分块 P_N 用零填充成完整大小的最后块 42。依赖于长期固定得初始化矢量 IV_0 和包有效载荷 26 的任何先前第一块序列中至少一个块，来生成一个初始化矢量 IV_N。可能会出现没有先前第一序列的情况。为了不在异或运算中直接将长期固定的初始化矢量 IV_0 作为操作数使用，首先通过使用加密密码 E_k 的反转作为解密密码，将所述 CW 作为密钥，来解密与完整大小的最后块 39 相关的初始化矢量 IV_N。通过应用块密码 E_k，获得对所述结果和完整大小的最后块 42 的异或，并对

其加密。其结果是完整大小的加扰块 43，其通过删除在大小和位置上对应于填充部分块 P_N 而添加的数据部分，而被截短。将保留的部分 C_N 插入加扰有效载荷 36。

[0115] 以这样的方式加扰一串 MPEG-2 TS 包 27 的有效载荷，从而形成加扰的数据流。密文挪用以及处理单个部分块的方法保证了加扰的有效载荷 36 在大小上等于原始明文 MPEG-2 TS 包 27 的有效载荷 26。因此，与明文 MPEG-2 TS 包 27 的报头相比，加扰的 MPEG-2 TS 包 34 的报头 35 基本上不需要修改，除非要指出它已经被加扰了，以及可选地奇数和偶数 CW 之一已被用于块密码 E_k。

[0116] 图 5 描述了对应于图 2 所描述的加扰操作的解扰操作。如同图 2 中的情况，图 5 基于在加扰的有效载荷 36 中准确地具有 N\M 个“超级块”的假设。加扰的有效载荷 36 组成了一串加扰数据块 C_i 序列，每个序列对应于一个“超级块”。描述出了加扰数据块 C_1-C_3 的第一序列 44 和块 C_{N-2}-C_N 的末尾序列 45。

[0117] 每个加扰数据块序列被分别解扰来形成相关的解扰数据块序列。因此，通过解扰块 C_1-C_3 的第一序列 44 来形成明文块 P_1-P_3 的第一序列 46。解扰块 C_{N-2}-C_N 的末尾序列 45 来形成明文块 P_{N-2}-P_N 的最后序列 47。明文块序列用来组成明文 MPEG-2 TS 包的有效载荷 48，前面是报头 49，从而组成重组的明文 MPEG-2 TS 包 50。

[0118] 通过对第一加扰数据块 C_1 应用作为编码密码 E_k 的反转的解密密码 D_K、以及应用以解密密码 D_K 的结果和加扰数据块序列 44 中下一个加扰块 C_2 作为操作数的异或算符，来获得第一明文块序列 46 中的第一解扰数据块 P_1。第二个块 P_2 也用相同的方式获得。从 ECM 所获得的 CW 用作解密密码 D_K 的密钥。

[0119] 通过向在加扰数据块 C_1-C_3 的第一序列 44 中最后一块 C_3 应用解密密码 D_K，来获得第一明文块序列 46 中的最后一个解扰数据块 P_3。将结果同与第一“超级块”相关的初始化矢量 IV_3 异或。这个初始化矢量 IV_3 的生成依赖于至少一个数据块，该至少一个数据块的获得是通过向相同序列中最后的加扰数据块 C_3 之前的第一加扰数据块序列 44 中的一个块应用解密密码 D_K、以及应用以至少具有解密密码 D_K 的结果和加扰数据块序列中下一位置上的解扰数据块为操作数的异或算符。在所描述的实施例中，初始化矢量 IV_3 是长期固定的初始化矢量 IV_0 和在最后的明文块 P_3 之前第一明文块序列 46 的所有块的异或。由于这些先前的明文块在最后的明文块 P_3 获得之前得出，所以该解扰方法是相对高效的。

[0120] 通常，在对包括在加扰有效载荷 35 中的加扰数据块序列串的每一个使用固定数目 M 个块的加扰数据的实施例，明文块按照如下方法建立：

[0121] $P_{j.M} = D_k[P_{j.M} \hat{} IV_{j.M}]$，

[0122] $P_{(j-1).M+i} = C_{(j-1).M+i+1} \hat{} D_k[C_{(j-1).M+i}]$，$i = M-1...1$，$j = 1...N\backslash M$。

[0123] 在所描述的实施例中，用于解密第 j 个序列中的块的初始化矢量 $IV_{j.M}$ 可以按照如下方法获得：

[0124] $IV_{j.M} = IV_0 \hat{} P_1 \hat{} ... P_i \hat{} P_{j.M-1}$。

[0125] 在该方法中，用于解密第二以及其它加扰数据块序列的初始化矢量的生成，依赖于由解扰加扰有效载荷 36 中的一个先前解扰数据块序列获得的解扰数据块序列中至少一个解扰数据块。

[0126] 图 6 描述了如果加扰的有效载荷 36 由整数 N\M 个第一基本块序列、以及在大小上等于基本块的整数倍以及基本块大小的一部分的后续数据量组成，那么如何进行加扰方

法。在所描述的实施例中，随后的数据量可以被分成两个完全加扰的块 C_{N-2}、C_{N-1} 以及一个部分块 C_N。最后的块 C_N 用零填充到与最后一个完整的基本块 51 相同的大小。因此，一个末尾序列由块 C_{N-2}、C_{N-1} 和最后一个完整的基本块 51 组成。通过向位于末尾加扰数据块序列的最后块之前紧邻的块 C_{N-1} 使用解密密码 D_k、对解密密码的结果和最后一个完整基本块 51 应用异或算符、以及删除对应于填充最后的加扰块 C_N 而增加的数据位置和大小的异或算符结果的一部分 C'，来形成最后的明文块 P_N。最后两个明文块 P_{N-1}，P_N 之前的每个任意块——在这种情况下，序列中的第一块 P_{N-2} 是唯一一个这种块——是通过向末尾加扰数据块序列中相应位置的块使用解密密码 D_k、以及对解密密码的结果和末尾加扰数据块序列下一位置的加扰数据块应用异或算符而获得的。

[0127] 通过向连接最后块 C_N 和对应于填充所用的零的大小和位置的所删除的部分 C' 而形成的块 52 应用解密密码、然后应用以解密密码的结果 D_k 和初始化矢量 IV_N 为操作数的异或算符，获得末尾明文块序列中最后块之前的块 P_{N-1}。作为初始化矢量 IV_N，初始化矢量是通过应用以初始化矢量 IV_0 和明文 MPEG-2 TS 包有效载荷 48 的最后两块 P_{N-1}，P_N 的每一个为操作数的异或算符来获得的。

[0128] 如果加扰的有效载荷 36 由 N\M 整数个加扰数据块以及随后在大小上少于一个基本块的数据量组成，就采取图 7 中描述的操作。一个部分加扰块 C_N 用零填充成完整大小的最后加扰块 53。依赖于长期固定的初始化矢量 IV_0 和加扰有效载荷 36 的任何先前加扰块序列中至少一个块来生成一个初始化矢量 IV_N。这可能会出现没有先前加扰块序列的情况。为了不在异或运算中直接将长期固定初始化矢量 IV_0 作为操作数使用，首先使用与块链接模式中所使用的相同的解密密码 D_k，将 CW 作为密钥，来解密与完整大小的最后块 53 相关的初始化矢量 IV_N。获得对上述结果和完整大小的加扰块 50 的异或。结果是完整大小的块 54，它通过删除在大小和位置上对应于填充部分加扰块 C_N 所添加数据的部分 C' 而被截短。将保留的部分 P_N 插入明文 MPEG-2 TS 包有效载荷。

[0129] 因此，已经详细描述了一种方法，其中“超级块”具有预定大小，但是可以配合可变大小的包有效载荷，包括不是选定大小的“超级块”的整数倍的那些包。用于每个“超级块”的初始化矢量从不直接用作异或算符的掩码。它尽可能地依赖于包有效载荷中的先前的明文块，所以实现了初始化矢量尽可能多的变化。对于加扰器和解扰器来说，操作结果的存储需求基本相同，并且出于安全原因考虑，可以通过选择较小长度的“超级块”来将存储需求保持在可接受的较低水平。

[0130] 本发明不限于所描述的实施例，其可以在后附的权利要求的范围内变化。特别地，实施例可能是第一加扰块序列没有通过在加扰器中反转块的顺序而转换成第二加扰块序列，但是在解扰器中，在执行在此所描述的解扰加扰数据流的方法之前，执行了反转。

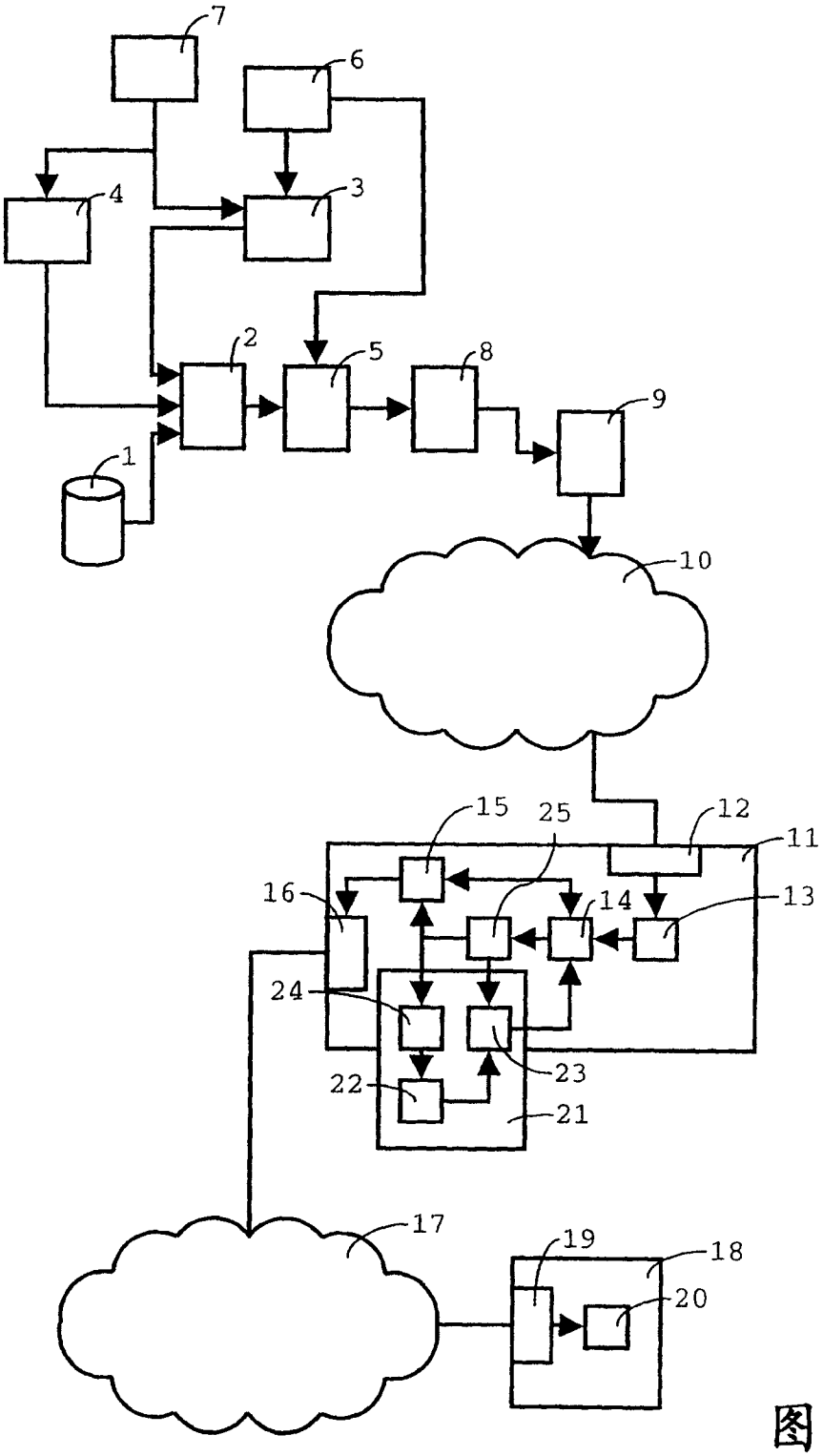


图1

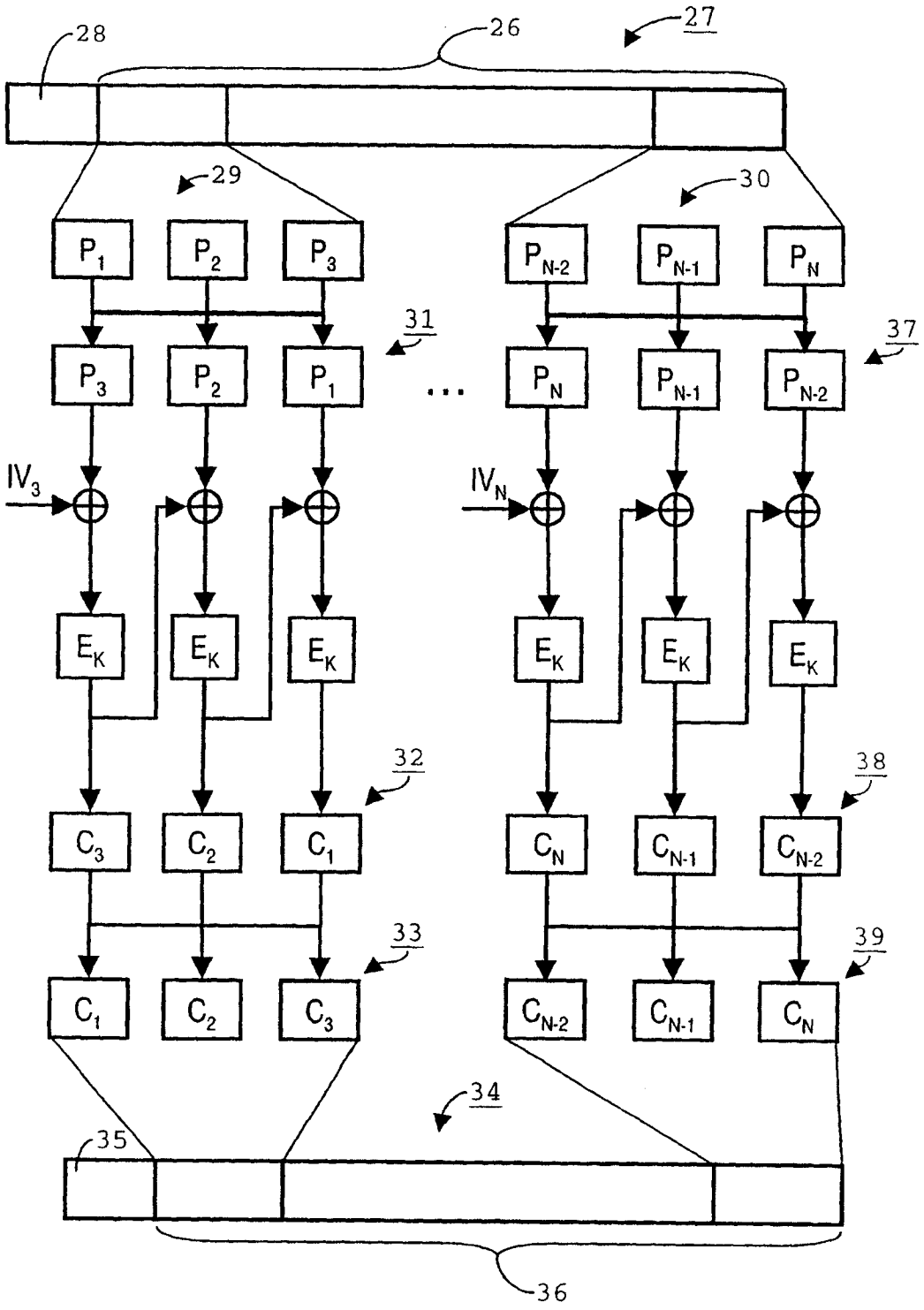

28
26
27
29
30
P1
P2
P3
PN-2
PN-1
PN
31
37
P3
P2
P1
...
PN
PN-1
PN-2
IV3
IVN
EK
EK
EK
EK
EK
EK
32
38
C3
C2
C1
CN
CN-1
CN-2
33
39
C1
C2
C3
CN-2
CN-1
CN
34
35
36

图 2

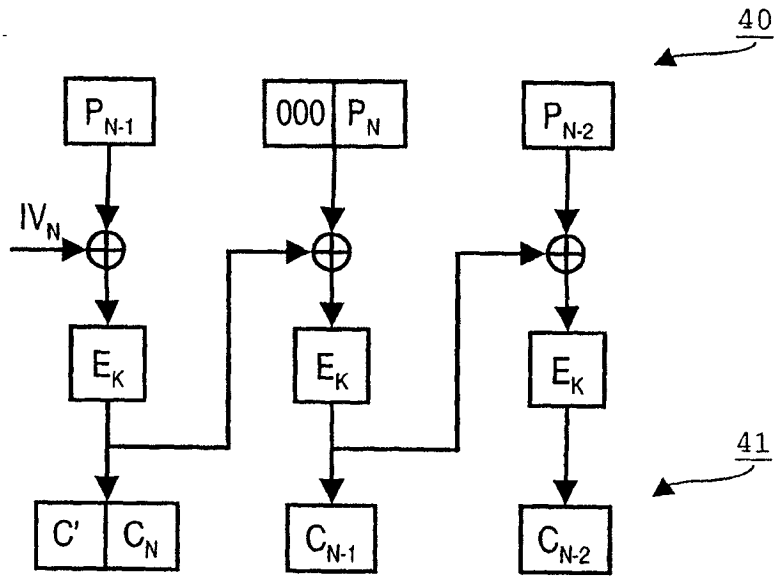

40
P_{N-1}
000 P_N
P_{N-2}
IV_N
E_K
E_K
E_K
41
C' C_N
C_{N-1}
C_{N-2}

图 3

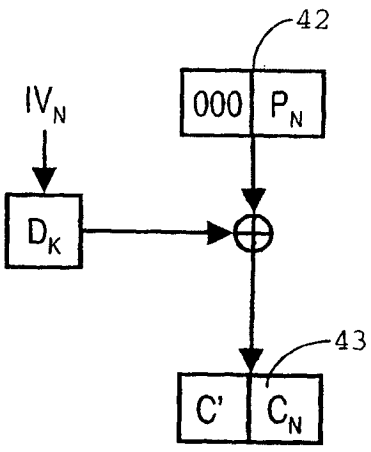

42
IV_N
000 P_N
D_K
43
C' C_N

图 4

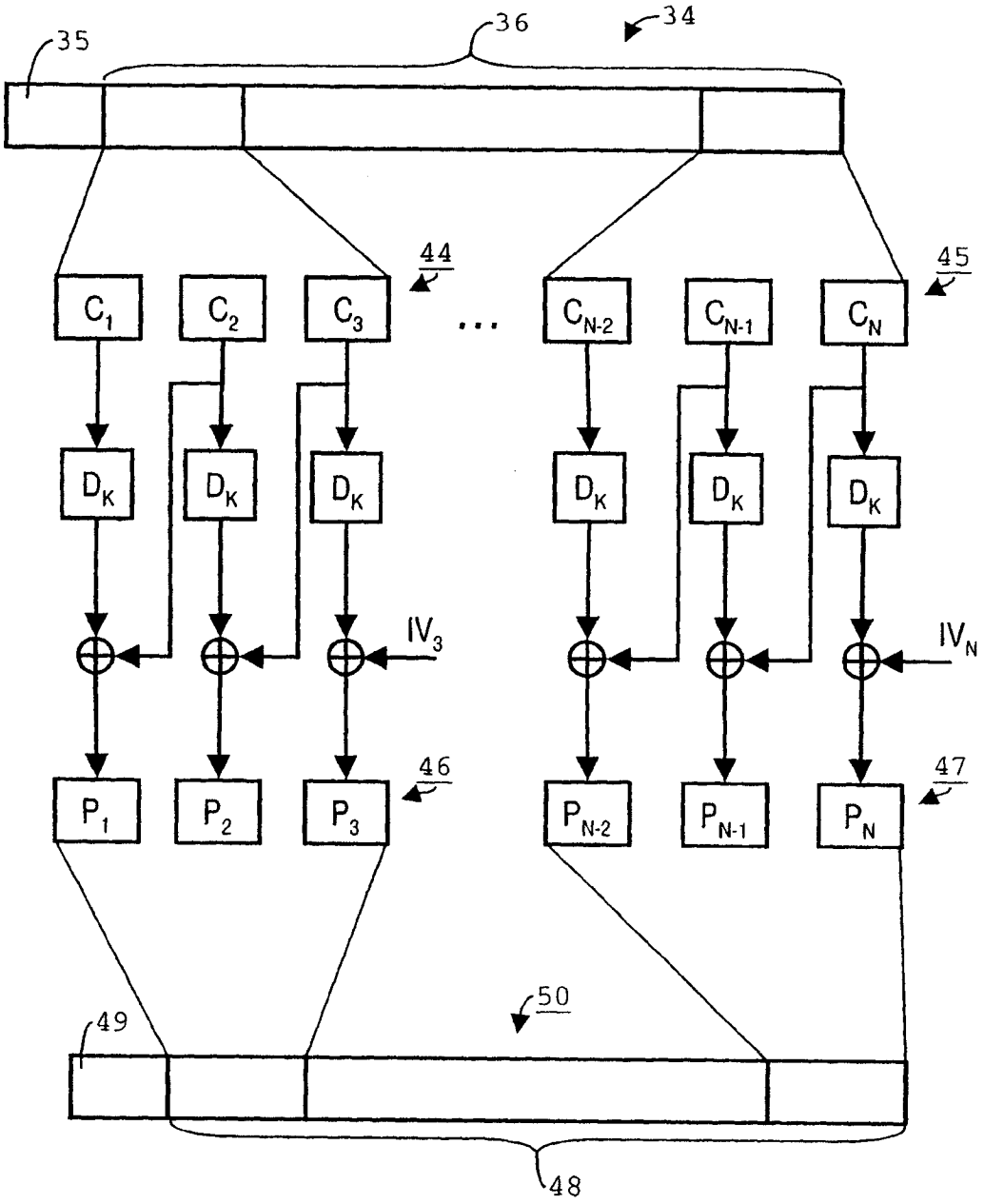

35
36
34
44
45
C1
C2
C3
CN-2
CN-1
CN
DK
IV3
IVN
46
47
P1
P2
P3
PN-2
PN-1
PN
49
50
48

图 5

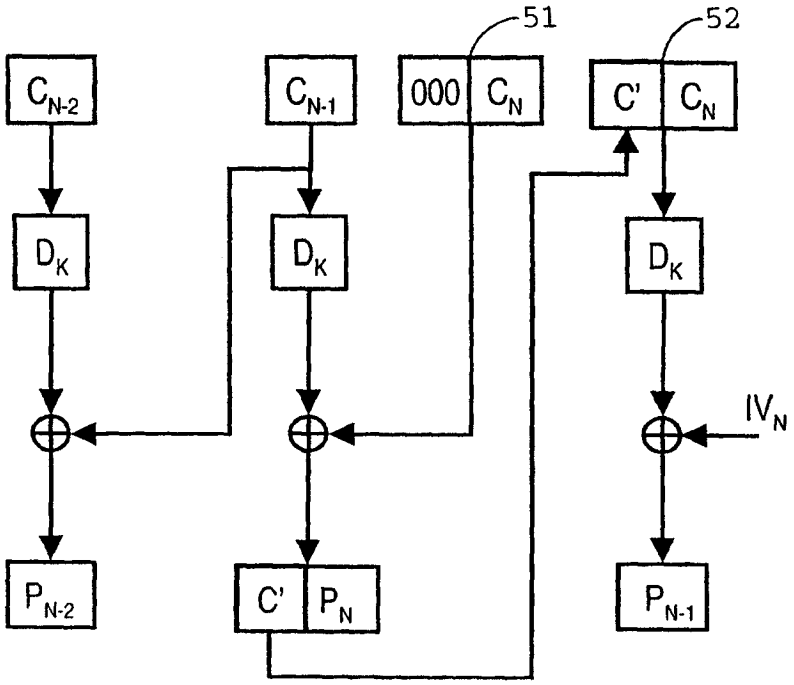

51
52
C_{N-2}
C_{N-1}
000 C_N
C' C_N
D_K
D_K
D_K
IV_N
P_{N-2}
C' P_N
P_{N-1}

图 6

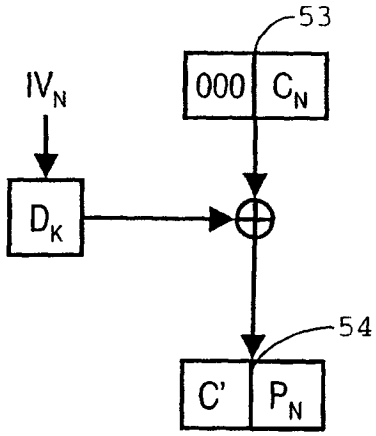

53
IV_N
000 C_N
D_K
54
C' P_N

图 7