(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 101061661 B
(45)授权公告日 2010.10.27

(21)申请号 200580031603.7

(22)申请日 2005.10.18

(30)优先权数据
60/620,877 2004.10.20 US
11/201,626 2005.08.10 US

(85)PCT申请进入国家阶段日
2007.03.20

(86)PCT申请的申请数据
PCT/US2005/037877 2005.10.18

(87)PCT申请的公布数据
WO2006/045038 EN 2006.04.27

(73)专利权人 思科技术公司
地址 美国加利福尼亚州

(72)发明人 大卫·A·麦格鲁 斯科特·弗吕尔

(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 9/28(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 1281607 A,2001.01.24, 全文.
CN 1486555 A,2004.03.31, 全文.
WO 2005/081934 A2,2005.09.09, 全文.
US 6061449 A,2000.05.09, 全文.
US 2003/0123667 A1,2003.07.03, 全文.

审查员 郑昊

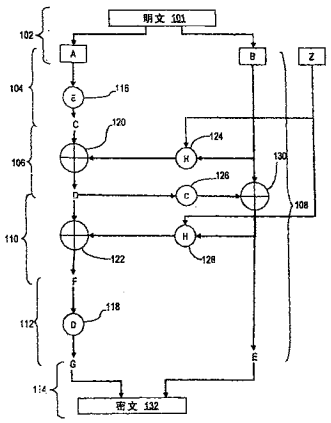
权利要求书 3 页 说明书 13 页 附图 5 页

(54)发明名称

加密方法

(57)摘要

运算的块密码模式实现具有任意块长度的块密码并且提供总是与输入明文大小相同的输出密文。该模式在不允许数据扩展的系统中可以提供最好的可能安全性,例如盘块加密和一些网络协议。该模式接受另外的输入,该输入可以用来保护不受通过重新布置密文块而操纵密文的攻击。来自用于块密码的运算的Galois/计数器模式的通用散列函数可以用在针对硬件和软件效率的实施例中。



CN 101061661 B

1. 一种数据通信方法，包括计算机实现的以下步骤：

在将发送器和接收器彼此耦合的电子数字电信链路上接收包括输入明文数据的第一消息；

将所述明文数据分离成第一明文数据段和第二明文数据段；

使用块密码加密和第一密钥对所述第一明文数据段加密，从而创建第一加密段；

对所述第一加密段和所述第二明文数据段与相关数据元素的基于第二密钥的散列施加排他性或运算，从而创建第一中间结果数据；

对所述第一中间结果数据和第三密钥施加加密运算，从而创建加密输出；

对所述加密输出和所述第二明文数据段施加排他性或运算，从而创建第二中间结果数据；

对所述第一中间结果数据和所述第二中间结果与所述相关数据元素的使用第四密钥的散列施加排他性或运算，从而创建第三中间结果数据；以及

创建所述第二中间结果数据和使用第五密钥对第三中间结果数据的解密结果的拼接作为输出密文；

将所述输出密文在第二消息中通过所述链路发送给所述接收器；

其中所述明文数据、段、中间结果数据、相关数据和密文中的每一项是存储在电子数字存储设备中的数字值；

其中所述分离、加密、施加和创建操作在耦合到所述电子数字存储设备并且与所述数字数据值交互的电子数字数据处理装置中执行。

2. 一种加密方法，包括计算机实现的以下步骤：

接收明文数据；

将所述明文数据分离成第一明文数据段 (A) 和第二明文数据段 (B)；

使用块密码加密和第一密钥对所述第一明文数据段 (A) 加密，从而创建第一加密段 (C)；

对所述第一加密段 (C) 和所述第二明文数据段 (B) 与相关数据元素 (Z) 的基于第二密钥的散列施加排他性或运算，从而创建第一中间结果数据 (D)；

对所述第一中间结果数据 (D) 和第三密钥施加加密运算，从而创建加密输出；

对所述加密输出和所述第二明文数据段 (B) 施加排他性或运算，从而创建第二中间结果数据 (E)；

对所述第一中间结果数据 (D) 和所述第二中间结果与所述相关数据元素 (Z) 的使用第四密钥的散列施加排他性或运算，从而创建第三中间结果数据 F；以及

创建所述第二中间结果数据 (E) 和使用第五密钥对第三中间结果数据 (F) 的解密结果的拼接作为输出密文。

3. 如权利要求 2 所述的方法，其中所述第二密钥、第三密钥、第四密钥和第五密钥是基于所述第一密钥和密钥导出过程而确定的。

4. 如权利要求 2 所述的方法，包括通过以相反的顺序执行权利要求 1 所述的步骤而对所述密文进行解密。

5. 如权利要求 2 所述的方法，其中所述明文包括存储在盘驱动设备中的数据块，所述方法还包括将所述密文存储在所述盘驱动设备中。

6. 如权利要求 2 所述的方法，其中所述明文包括符合不可扩展数据协议的分组的数据净荷，所述方法还包括将所述密文存储在所述分组中。

7. 如权利要求 2 所述的方法，其中所述明文包括符合安全实时协议的分组的数据净荷，所述方法还包括将所述密文存储在所述分组中。

8. 如权利要求 2 所述的方法，其中所述加密运算是 AES 计数器模式加密。

9. 一种计算机装置，包括：

用于接收明文数据的装置；

用于将所述明文数据分离成第一明文数据段和第二明文数据段的装置；

用于使用块密码加密和第一密钥对所述第一明文数据段加密，从而创建第一加密段的装置；

用于对所述第一加密段和所述第二明文数据段与相关数据元素的基于第二密钥的散列施加排他性或运算，从而创建第一中间结果数据的装置；

用于对所述第一中间结果数据和第三密钥施加计数器模式的加密运算，从而创建计数器模式的输出的装置；

用于对所述计数器模式的输出和所述第二明文数据段施加排他性或运算，从而创建第二中间结果数据的装置；

用于对所述第一中间结果数据和所述第二中间结果与所述相关数据元素的使用第四密钥的散列施加排他性或运算，从而创建第三中间结果数据的装置；以及

用于创建所述第二中间结果数据和使用第五密钥对第三中间结果数据的解密结果的拼接作为输出密文的装置。

10. 如权利要求 9 所述的装置，其中所述第二密钥、第三密钥、第四密钥和第五密钥是基于所述第一密钥和密钥导出过程而确定的。

11. 如权利要求 9 所述的装置，包括通过以相反的顺序执行权利要求 1 所述的步骤而对所述密文进行解密。

12. 如权利要求 9 所述的装置，其中所述明文包括存储在盘驱动设备中的数据块，所述装置还将所述密文存储在所述盘驱动设备中。

13. 如权利要求 9 所述的装置，其中所述明文包括符合不可扩展数据协议的分组的数据净荷，所述装置还将所述密文存储在所述分组中。

14. 如权利要求 9 所述的装置，其中所述明文包括符合安全实时协议的分组的数据净荷，所述装置还将所述密文存储在所述分组中。

15. 如权利要求 9 所述的装置，其中所述加密运算是 AES 计数器模式加密。

16. 一种加密装置，包括：

网络接口，该网络接口耦合到用于从其接收一个或多个分组流的数据网络；

处理器；

接收逻辑，所述接收逻辑耦合到所述处理器并被配置为接收明文数据；

分离逻辑，所述分离逻辑耦合到所述处理器并被配置为将所述明文数据分离成第一明文数据段 (A) 和第二明文数据段 (B)；

加密逻辑，所述加密逻辑耦合到所述处理器并被配置为使用块密码加密和第一密钥对所述第一明文数据段 (A) 加密，从而创建第一加密段 (C)；

第一施加逻辑，所述第一施加逻辑耦合到所述处理器并被配置为对所述第一加密段 (C) 和所述第二明文数据段 (B) 与相关数据元素 (Z) 的基于第二密钥的散列施加排他性或运算，从而创建第一中间结果数据 (D)；

第二施加逻辑，所述第二施加逻辑耦合到所述处理器并被配置为对所述第一中间结果数据 (D) 和第三密钥施加加密运算，从而创建加密输出；

第三施加逻辑，所述第三施加逻辑耦合到所述处理器并被配置为对所述加密输出和所述第二明文数据段 (B) 施加排他性或运算，从而创建第二中间结果数据 (E)；

第四施加逻辑，所述第四施加逻辑耦合到所述处理器并被配置为对所述第一中间结果数据 (D) 和所述第二中间结果与所述相关数据元素 (Z) 的使用第四密钥的散列施加排他性或运算，从而创建第三中间结果数据 (F)；以及

创建逻辑，所述创建逻辑耦合到所述处理器并被配置为创建所述第二中间结果数据 (E) 和使用第五密钥对第三中间结果数据 (F) 的解密结果的拼接作为输出密文。

17. 如权利要求 16 所述的装置，其中所述第二密钥、第三密钥、第四密钥和第五密钥是基于所述第一密钥和密钥导出过程而确定的。

18. 如权利要求 16 所述的装置，包括通过以相反的顺序执行权利要求 1 所述的步骤而对所述密文进行解密。

19. 如权利要求 16 所述的装置，其中所述明文包括存储在盘驱动设备中的数据块，所述装置还将所述密文存储在所述盘驱动设备中。

20. 如权利要求 16 所述的装置，其中所述明文包括符合不可扩展数据协议的分组的数据净荷，所述装置还将所述密文存储在所述分组中。

21. 如权利要求 16 所述的装置，其中所述明文包括符合安全实时协议的分组的数据净荷，所述装置还将所述密文存储在所述分组中。

22. 如权利要求 16 所述的装置，其中所述加密运算是 AES 计数器模式加密。

23. 一种将明文加密成密文的方法，该方法包括计算机实现的以下步骤：

接收所述明文和辅助数据值；

将所述明文分离成第一明文部分和第二明文部分；

对所述第一明文部分加密以创建第一中间值；

使用 GF(2^{128}) 上的通用散列函数从所述第二明文部分和所述辅助数据值产生第一散列值，并将所述第一散列值与所述第一中间值组合以创建第二中间值；

对所述第二中间值进行计数器模式加密以产生加密输出，并将所述第二明文部分与所述加密输出组合以创建第一密文部分；

从所述第一密文部分和所述辅助数据值产生第二散列值，并将所述第二散列值与所述第二中间值组合以创建第三中间值；

对第三中间值解密以创建第二密文部分；以及

基于所述第一密文部分和所述第二密文部分的拼接创建并存储所述密文。

加密方法

技术领域

[0001] 本发明一般涉及数据处理。更具体地说，本发明涉及计算机实现的密码学。

背景技术

[0002] 该部分中所描述的方法可以被实现，但不是一定是以前被构思或实现的方法。因此，除非在这里另外指示，该部分中所描述的方法对于本申请中的权利要求来说不是现有技术，并且不承认通过包括在该部分中而成为现有技术。

[0003] 如果密文 (ciphertext) 与明文 (plaintext) 具有完全相同的位数，则加密方法是长度保留的。这样的方法必须是确定性的，因为密文内不可能容纳随机数据（例如初始化向量）。此外，确定性的长度保留加密也适合于某些应用。例如，在一些加密的数据库应用中，确定性对于确保查找操作中的明文值完全对应于以前存储的明文值来说是必不可少的。

[0004] 此外，在密码学的一些应用中，不可能提供某些希望的安全服务，例如关于数据的消息认证，因为不可能将数据扩展为包括消息认证码。例如，一些网络（例如一些无线网络情况）中的安全实时协议 (SRTP) 不能扩展明文数据。长度保留算法实质上实现密码本；用相同的密钥对相同的明文进行重复的加密产生同样的密文。对手通过察看哪些密文值匹配而得知明文。尽管如此，在一些情况中，长度保留加密仍然是有用的。例如，长度保留可以使加密被引入到已经实现和运用的数据处理系统中，或者在具有固定宽度字段的协议中或在限制数据扩展的允许量的系统中使用。在这些情况中，希望一种长度保留的、确定性的、无展性的加密方法作为消息认证的替换。

[0005] 非正式地，如果改变密文值的单个位影响相应明文的所有位，则密码是无展性的。因此，在无展性的加密中，不可能通过操纵密文来操纵解密之后出现的明文。更正式地，希望的无展性密码实现伪随机排列；其对于有限计算的对手而言与消息组的排列没有区别。希望这样的密码能够处置可变大小的明文，因此需要提供伪随机的任意长度排列的密码：对于每个可能的明文长度，密码充当伪随机排列。

[0006] 无展性加密是传统运算模式（例如密码块链和计数器模式加密）上的很大改善，传统运算模式在任何时候都不能增加消息认证标签。另外，无展性密码也可以接受可以用来防止密文置换攻击的另外输入值。例如，SRTP 序号可以被用在与运行 SRTP 的网络元件相关联的实现方式中。

[0007] 无展性加密对于盘块 (disk block) 加密也是有用的。这样的加密经常被用在远程存储系统中，因为它允许存储区域网络被用在网络管理员仅在有限程度的上被信任的应用中。

[0008] 在理论文献中存在很多无展性密码提议。这里所公开的方法的一个实施例可以被称为用于块密码 (block cipher) 的运算的延伸密码本 (XCB) 模式，它在数个方面上不同于现有技术。由 Luby 和 Rackoff 在 20 世纪 80 年代所提出的密码（这里称为“LR”）为很多过去的技术提供无展性密码的理论基础。XCB 与该技术的不同之处在于使用不同组的计算；

XCB 不是 Fesitel 密码，而 LR 是。XCB 依赖于块密码的可逆性，而 LR 不是。而且，LR 需要四轮以确保安全，而 XCB 三轮就是安全的。

[0009] 在 20 世纪 90 年代，Naor 和 Reingold 公布了一些基本思想上的优化，如在“On the Construction of Pseudo-Random Permutations：Luby Rackoff Revisited”中的描述。虽然该技术使用四轮，但是第一轮和第四轮是 Naor 和 Reingold 所定义的“两两独立”排列。Naor-Reingold 方法也不依赖于块密码的可逆性。该设计完全不同于 XCB，XCB 仅使用三轮、不使用两两独立排列并且依赖于块密码的可逆性。

[0010] 在 20 世纪 90 年代，Stefan Lucks 在“Faster Luby-Rackoff Ciphers”中描述了散列函数的使用。Anderson 和 Biham 也发表了一些类似的技术，示出了两种密码 BEAR 和 LION。该技术仅讨论了 LR 构造，并且不依赖于块密码的可逆性。此外，它需要四轮以确保安全。

[0011] 更近一些的时候，Patel、Ramzan 和 Sundaram 发表了两篇延伸 Naor-Reingold 技术的论文，“Towards Making Luby-Rackoff Ciphers Optimal and Practical”和“Luby-Rackoff Ciphers over Finite Algebraic Structures or Why XOR is not so Exclusive”。该技术基于 Naor-Reingold 技术，并且用于该技术的所有注解都适用于这些设计。

[0012] Bellare 和 Rogaway 在“On the Construction of Variable-Input-Length Ciphers”中描述了一种是长度保留但不是无展性的运算模式。他们将该技术称为 VIL，它与 XCB 大不相同。

[0013] Rogaway 和 Halevi 在“The EMD Mode of Operation(A Tweaked,Wide-Blocksize, Strong PRP)”和“EME？：extending EME to handle arbitrary-length messages with associated data”中设计了是无展性的 EME 运算模式。虽然该技术的目标与 XCB 的目标相同，但是 EME 的设计不同于 XCB 的设计。重要的是，EME 对块密码的调用是 XCB 的两倍。

[0014] 独立地，McGrew 和 Viega 向 IEEE 存储安全工作组 (IEEE Security in Storage Working Group) 提交了称为 ABL（任意块长度模式）的优化 Luby-Rackoff 设计。XCB 与 ABL 大不相同。

[0015] Patel 等人发表了描述两种密码构造的标题为“Efficient Constructions of Variable-Input-Length Block Ciphers”的论文。第 3 部分中的方法被这样构建：不能并行完成散列调用和（第 1 轮）和块密码调用（第 2 轮）。与此相反，在 XCB 中，前两轮可以并行完成。XCB 同时进行这些运算的能力对于高速硬件实现来说是很大的性能好处。此外，第 3 部分的密码在第 3 轮中所使用的“计数器模式”之外，仅具有单个散列函数应用和单个块密码调用。由此，对于选择的明文 / 密文攻击来说不安全。因此，第 3 部分中的方法仅提供伪随机排列，而不是“超级伪随机排列”。与此相反，XCB 具有两个散列调用和两个块密码调用，是超级伪随机排列。

发明内容

[0016] 本发明的一方面包括一种数据通信方法，该数据通信方法包括计算机实现的以下步骤：在将发送器和接收器彼此耦合的电子数字电信链路上接收包括输入明文数据的第一消息；将明文数据分离成第一明文数据段和第二明文数据段；使用块密码加密和第一密钥

对第一明文数据段加密，从而创建第一加密段；对第一加密段和第二明文数据段与相关数据元素的基于第二密钥的散列施加排他性或运算，从而创建第一中间结果数据；对第一中间结果数据和第三密钥施加加密运算，从而创建加密输出；对加密输出和第二明文数据段施加排他性或运算，从而创建第二中间结果数据；对第一中间结果数据和第二中间结果与相关数据元素的使用第四密钥的散列施加排他性或运算，从而创建第三中间结果数据；以及创建第二中间结果数据和使用第五密钥对第三中间结果数据的解密结果的拼接作为输出密文；将输出密文在第二消息中通过链路发送给接收器。其中，明文数据、段、中间结果数据、相关数据和密文中的每一项是存储在电子数字存储设备中的数字值，并且分离、加密、施加和创建操作在耦合到电子数字存储设备并且与数字数据值交互的电子数字数据处理装置中执行。

[0017] 本发明的另一方面包括一种加密方法，该加密方法包括计算机实现的以下步骤：接收明文数据；将明文数据分离成第一明文数据段 (A) 和第二明文数据段 (B)；使用块密码加密和第一密钥对第一明文数据段 (A) 加密，从而创建第一加密段 (C)；对第一加密段 (C) 和第二明文数据段 (B) 与相关数据元素 (Z) 的基于第二密钥的散列施加排他性或运算，从而创建第一中间结果数据 (D)；对第一中间结果数据 (D) 和第三密钥施加加密运算，从而创建加密输出；对加密输出和第二明文数据段 (B) 施加排他性或运算，从而创建第二中间结果数据 (E)；对第一中间结果数据 (D) 和第二中间结果与相关数据元素 (Z) 的使用第四密钥的散列施加排他性或运算，从而创建第三中间结果数据 F；以及创建第二中间结果数据 (E) 和使用第五密钥对第三中间结果数据 (F) 的解密结果的拼接作为输出密文。

[0018] 本发明的另一方面包括一种计算机装置，包括：用于接收明文数据的装置；用于将明文数据分离成第一明文数据段和第二明文数据段的装置；用于使用块密码加密和第一密钥对第一明文数据段加密，从而创建第一加密段的装置；用于对第一加密段和第二明文数据段与相关数据元素的基于第二密钥的散列施加排他性或运算，从而创建第一中间结果数据的装置；用于对第一中间结果数据和第三密钥施加计数器模式的加密运算，从而创建计数器模式的输出的装置；用于对计数器模式的输出和第二明文数据段施加排他性或运算，从而创建第二中间结果数据的装置；用于对第一中间结果数据和第二中间结果与相关数据元素的使用第四密钥的散列施加排他性或运算，从而创建第三中间结果数据的装置；以及用于创建第二中间结果数据和使用第五密钥对第三中间结果数据的解密结果的拼接作为输出密文的装置。

[0019] 本发明的另一方面包括一种加密装置，包括：网络接口，该网络接口耦合到用于从其接收一个或多个分组流的数据网络；处理器；接收逻辑，接收逻辑耦合到处理器并被配置为接收明文数据；分离逻辑，分离逻辑耦合到处理器并被配置为将明文数据分离成第一明文数据段 (A) 和第二明文数据段 (B)；加密逻辑，加密逻辑耦合到处理器并被配置为使用块密码加密和第一密钥对第一明文数据段 (A) 加密，从而创建第一加密段 (C)；第一施加逻辑，第一施加逻辑耦合到处理器并被配置为对第一加密段 (C) 和第二明文数据段 (B) 与相关数据元素 (Z) 的基于第二密钥的散列施加排他性或运算，从而创建第一中间结果数据 (D)；第二施加逻辑，第二施加逻辑耦合到处理器并被配置为对第一中间结果数据 (D) 和第三密钥施加加密运算，从而创建加密输出；第三施加逻辑，第三施加逻辑耦合到处理器并被配置为对加密输出和第二明文数据段 (B) 施加排他性或运算，从而创建第二中间结果数据

(E) ;第四施加逻辑,第四施加逻辑耦合到处理器并被配置为对第一中间结果数据 (D) 和第二中间结果与相关数据元素 (Z) 的使用第四密钥的散列施加排他性或运算,从而创建第三中间结果数据 (F) ;以及创建逻辑,创建逻辑耦合到处理器并被配置为创建第二中间结果数据 (E) 和使用第五密钥对第三中间结果数据 (F) 的解密结果的拼接作为输出密文。

[0020] 本发明的另一方面包括一种将明文加密成密文的方法,该方法包括计算机实现的以下步骤 :接收明文和辅助数据值 ;将明文分离成第一明文部分和第二明文部分 ;对第一明文部分加密以创建第一中间值 ;使用 GF(2^{128}) 上的通用散列函数从第二明文部分和辅助数据值产生第一散列值,并将第一散列值与第一中间值组合以创建第二中间值 ;对第二中间值进行计数器模式加密以产生加密输出,并将第二明文部分与加密输出组合以创建第一密文部分 ;从第一密文部分和辅助数据值产生第二散列值,并将第二散列值与第二中间值组合以创建第三中间值 ;对第三中间值解密以创建第二密文部分 ;以及基于第一密文部分和第二密文部分的拼接创建并存储密文。

附图说明

[0021] 本发明是通过示例而不是限制的方式来说明的,在附图的图形中,相似的标号指的是类似的元件,其中 :

[0022] 图 1A 是提供可以使用这里的方法的通信系统模型的框图 ;

[0023] 图 1B 是示出了根据一个实施例的加密过程的步骤和元件的数据流程图 ;

[0024] 图 2A 是第二实施例的加密运算的框图 ;

[0025] 图 2B 是乘法运算的框图 ;

[0026] 图 3A 是示出安全电信系统的框图 ;

[0027] 图 3B 是示出安全存储管理系统的框图 ;

[0028] 图 4 是示出了本发明的实施例可以在上面实现的计算机系统的框图。

具体实施方式

[0029] 描述了一种用于加密的方法和装置。在下面的描述中,为了说明的目的,给出了许多具体细节以提供对本发明的全面理解。然而,本领域技术人员将清楚本发明可以在没有这些具体细节的情况下实现。此外,公知的结构和器件用框图示出以避免不必要地模糊本发明。

[0030] 这里根据下面的提纲来描述实施例 :

[0031] 1.0 概述

[0032] 2.0 概念模型和目标

[0033] 3.0 用于块密码的运算的延伸密码本 (XCB) 模式

[0034] 3.1 运算原理

[0035] 3.2 应用示例

[0036] 3.3 安全性证明

[0037] 3.4 与现有方法的某些差别

[0038] 4.0 实现机制——硬件概述

[0039] 5.0 延伸和替换

[0040] …

[0041] 1.0 概述

[0042] 在上述背景中所确定的需要以及将从下面的描述中变得清楚的其他需要和目标可以在本发明中实现，本发明一方面包括加密方法，该加密方法包括计算机实现的接收明文数据的步骤；将明文数据分成第一明文数据段 A 和第二明文数据段 B；用块密码加密和第一密钥加密第一明文数据段 A，从而创建第一加密段 C；对第一加密段 C 和第二明文数据段 B 与相关数据元素 Z 的基于第二密钥的散列施加排他性 (exclusive)OR(或) 运算，从而创建第一中间结果数据 D；对第一中间结果数据 D 和第三密钥施加加密运算，从而创建加密输出；对加密输出和第二明文数据段 B 施加排他性 OR 运算，从而创建第二中间结果数据 E；对第一中间结果数据 D 和第二中间结果与相关数据元素 Z 的使用第四密钥的散列施加排他性 OR 运算，从而创建第三中间结果数据 F；以及创建第二中间结果数据 E 和使用第五密钥对第三中间结果数据 F 的解密结果的拼接作为输出密文。

[0043] 这里所规定的数据值标签在该描述仅仅是为了清楚和方便，另外可以是任意的；实施例和实现方式可以使用任何形式的标记或命名用于所述数据值。

[0044] 在一个特征中，第二密钥、第三密钥、第四密钥和第五密钥是基于第一密钥和密钥导出过程而确定的。在另一特征中，对密文进行解密涉及以相反的顺序执行上面的步骤。在另一特征中，明文包括存储在非易失性存储器中的数据块，密文存储在非易失性存储器中。另外或者可替换地，明文包括存储在盘驱动设备中的数据块，密文存储在盘驱动设备中。

[0045] 在另一特征中，明文包括符合不可扩展数据协议的分组的数据净荷，密文存储在分组中。在另一特征中，明文包括符合安全 RTP 的分组的数据净荷，密文存储在分组中。

[0046] 在各种特征中，用来从 C 计算 D 和用于从 D 计算 F 的加密运算可以是 AES 计数器模式加密或者 AES OFB 块密码模式。

[0047] 在其他方面中，本发明包括计算机装置和被配置为实现上述步骤的计算机可读介质。

[0048] 在这些方法中，运算的块密码模式实现具有任意块长度的块密码并且提供总是与输入明文大小相同的输出密文。该模式在不允许数据扩展的系统中可以提供最好的可能安全性，例如盘块加密和一些网络协议。该模式接受另外的输入，该输入可以用来保护不受通过重新布置密文块而操纵密文的攻击。来自用于块密码的运算的 Galois/ 计数器模式的通用散列函数可以用在实施例中以获得硬件和软件的高效率。

[0049] 2.0 概念模型和目标

[0050] 图 1A 是提供可以使用这里的方法的通信系统模型的框图。第一节点 Alice 通过不安全的通信链路 L 耦合到第二节点 Bob。Alice 和 Bob 不知道的是，第三节点 Frank 可以截取在链路 L 上发送的消息。

[0051] Alice 发送给 Bob 一系列消息，每个消息都与某些另外的数据 Z 相关联，数据 Z 可以包含当前时间 (nonce)，并且可以包含关于消息如何被网络和发送者与接收者之间的其他中间系统路由、处理或处置的信息。Alice 使用秘密密钥 K 并且使用 Z 作为加密函数的辅助输入对明文消息 P 加密，产生密文 C。Alice 在链路 L 上将 C 发送给 Bob；然而，Frank 截取 C 并将替代消息 C' 发送给 Bob。消息 C' 在 Frank 不改变密文的情况下等于 C。Bob 使用与 Alice 共享的秘密密钥 K 和相关数据的值 Z，利用解密函数将 C' 解密为 P'。Z 或者包含

在消息的非密文部分中，或者可以被推断出。如果 C' = C，那么 P' = P；否则，可以预期 P' 是随机的。

[0052] 如果加密函数和解密函数分别用 E 和 D 表示，那么通过符号，图 1A 的模型和之前的序列可以表示为：

[0053] C = E(K, Z, P)

[0054] P = D(K, Z, C)

[0055] 如果只要 C' ≠ C 或 Z' ≠ Z，值 P' = D(K, C', Z') 就是随机的，则在 C 和 E 中所使用的密文就是安全的。因此，任何对密文的改变都从而密文解密成不可预见的随机值，这些不可预见的随机值不传达有用的信息或明文。

[0056] 支持该模型的加密方法的实现方式一般具有下列目标：

[0057] ■具有与明文大小完全相同的密文；

[0058] ■加密任何大小的缓冲器的能力，即，加密任何大于零的位数的能力；

[0059] ■具有在密文或相关数据被操纵的情况下随机的解密输出；

[0060] ■需要固定宽度的块密码作为唯一的密码基元 (cryptographic primitive)。

[0061] 此外，创建这样的加密方法的商业实现方式的人可以另外具有下列目标，这些目标在实施例中是希望但不是必需的：

[0062] ■在标准假设下具有强力的、证明是安全的边界 (bound)；

[0063] ■具有最小的计算成本，并且

[0064] ■支持最大的并行化。

[0065] 3.0 用于块密码的运算的延伸密码本 (XCB) 模式

[0066] 3.1 运算原理——第一实施例——每轮密钥

[0067] 根据一个实施例，运算的延伸密码本模式充当具有相关数据的任意长度块密码。为了清楚说明示例的目的，这里的描述假设使用 128 位的块密码。如果定义适当大小的有限域 (field)，则实施例可以使用其他块密码宽度。

[0068] 图 1B 是示出了根据一个实施例的加密过程的步骤和元件的数据流程图。一般来说，图 1B 的过程接收用于加密的信息，并且用图 1B 中所示的计算操作和转换对这样的明文 101 加密，从而创建输出密文 132。明文 101 和密文 132 都可以包括任何形式的数据表示，例如位串、盘存储块等。

[0069] 如图 1B 可见，在步骤 102，明文 101 被分成 A 和 B 所表示的两部分。在一个实施例中，对于大小至少为 256 位的明文，明文 101 被分成两半 A 和 B，其中 A 是明文的第一个 128 位，B 是明文的剩余部分。还接收到另外的数据值 Z。另外的值 Z 可以以清晰的形式接收，并且可以包括任何辅助输入值。另外的值 Z 可以具有任何长度。该方法防止了一些依赖于密码本属性的攻击，因为用不同的 Z 值加密相同的明文值产生无关的密文值。在一个用于加密存储信息的实施例中，Z 是盘块编号。在用于网络通信的一个实施例中，Z 可以是消息序号，在这样的实施例中，Z 的使用可以保护不受重放攻击。

[0070] 在步骤 104，A 部分被用加密运算 116 和第一密钥值加密以产生第一中间值 C。用符号表示，步骤 104 为：$C \leftarrow E(K_0, A)$。

[0071] 在步骤 106，用第一 XOR 运算 120 和第一散列运算 124 计算第二中间值 D：$D \leftarrow C \text{ XOR } H(K_1, B, Z)$。在该表达式中，H 是散列函数。在一个实施例中，由 Galois 在用于块密码

的运算的 Galois/ 计数器模式 (GCM) 中所定义的 GHASH 算法可以被用于散列运算 124 和 128 中的散列算法。GCM 散列函数的使用提供硬件和软件两者上的效率并且考虑了现有的实现努力的潜在再使用。在其他实施例中，任何伪随机散列函数可以被用于散列运算 124 和 128。

[0072] 在步骤 108，使用第二 XOR 运算 130 和加密运算 126 计算第一密文部分 E：$E \leftarrow B$ XOR $CTR(K_2, D)$。在一个实施例中，CTR 和加密运算 126 包括高级加密标准 (AES) 计数器模式加密的使用。在另一实施例中，OFB 可以在步骤 108 使用并且可以用于加密运算 126；OFB 是运算的四种 DES 模式之一。当使用计数器模式时，计数器模式加密运算被配置为产生大小与目标数据相同的输出，如接下来所述，用 XOR 运算将计数器模式输出结合到该输出中。在可替换的实施例中，运算 126 可以是任何的块密码。

[0073] 在步骤 110，用第二散列函数 128 和第三 XOR 运算 122 计算第三中间值 F：$F \leftarrow D$ XOR $H(K_3, E, Z)$。第二散列运算 128 和在之前的表达式中的 H 与步骤 106 中所使用的是同一散列函数。在步骤 112，使用解密运算 118 确定第二密文部分 G，如 $G \leftarrow D(K_4, F)$。

[0074] 在步骤 114，通过拼接 G 和 E 而创建完整的密文 132。所产生的密文 132 可以被存储在网络协议消息中，存储在盘存储设备中或者用于各种其他的基于计算机的应用。使用这里的方法，密文 132 与明文 101 具有相同的长度。

[0075] 在该描述中，E 表示用作为集合 $\{0,1\}^k$ 的元素的密钥 K 对作为集合 $\{0,1\}^w$ 的元素的值 X 进行块密码加密，D(K,X) 表示用作为集合 $\{0,1\}^k$ 的元素的密钥 K 对作为集合 $\{0,1\}^w$ 的元素的值 X 进行块密码解密。除了三轮以相反的顺序运行之外，解密运算 D 与加密运算 E 相同。

[0076] 加密运算 116 和解密运算 118 可以包括任何伪随机排列；它们不需要具有如加密和解密运算的关系。加密运算 116 和解密运算 118 可以以硬件、软件、固件或组合的形式实现。在一硬件实现方式中，如果密钥 K_1 和 K_4 在各自的运算中被倒置，则相同的电路可以实现加密运算 116 和解密运算 118 两者。此外，在另一实施例中，加密运算 116 和解密运算 118 每个都可以包括任何的伪随机排列操作并且不需要具有加密 - 解密关系。

[0077] 这里所描述的密钥 K_0 至 K_4 中的每一个密钥可以包括第一密钥和多个从第一密钥通过数学方法或通过计算导出的其他密钥。在该方法中，在加密开始前需要较少的密钥共享操作。或者，使用任何已知的密钥分配机制，可以预先将所有密钥提供给参与的处理元件。

[0078] 3.2 第二实施例——单个密钥

[0079] 根据另一实施例，虽然运算的延伸密码本模式充当具有相关数据的任意长度块密码，但是使用单个密钥而不是每轮一个密钥。图 2A 是第二实施例的加密运算的框图，图 2B 是乘法运算的框图。为了清楚说明示例的目的，这里的描述假设使用 128 位的块密码。如果定义适当大小的有限域，则实施例可以使用其他块密码宽度。

[0080] 第二实施例中所使用的两个主函数是域 $GF(2^{128})$ 上的块密码加密和乘法。在下面的算法描述中，用密钥 K 对值 X 所进行的块密码加密表示为 e(K, X)，块密码解密表示为 d(K,X)。符号 E 和 D 表示根据这里所描述的运算的延伸密码本模式的加密和解密。

[0081] 块密码输入和输出中的位数用 w 表示。当使用 AES 时，w 的值为 128。两个元素 X 和 $Y \in GF(2^{128})$ 的乘法表示为 $X \bullet Y$，X 和 Y 的加法表示为 $X \oplus Y$。该域中的加法相当于按位

的排他性或运算。在下面的独立部分中定义示例乘法运算。

[0082] 在算法描述中，函数 len(S) 返回 64 位的串，该串包含描述函数的自变量 S 中的位数的非负整数，最低有效位在右边。表达式 0^1 表示 1 个零的位串，A||B 表示两个位串 A 和 B 的拼接。位串被认为是从左边开始索引的，因此 S 的第零位是最左边的位。当 S 是位串并且 0 <= a < b <= len(S) 时，S[a ;b] 表示 S 的长度为 b-a 的子串，该子串由 S 的 a 至 b 位组成。符号 {} 表示具有零长度的位串。

[0083] 延伸密码本加密运算在表 1 中定义，解密运算在表 2 中定义，加密运算也在图 2A 中示出。表 1 和表 2 的算法使用块密码加密函数 e 和 d 以及散列函数 h 和伪随机函数 c。如图 2B 所示，变量 H、I、J 和 L 是通过在计数器模式下运行函数 e 而从 K 导出的。可选地，变量 H、I、J 和 L 的值在算法的赋值之间存储，从而为降低计算负荷折衷选择少量存储。

[0084] 表 1-XCB 加密运算

[0085] 给出密钥 $K \in \{0,1\}^k$，明文 $P \in \{0,1\}^m$，其中 $m \in [w, 2^{39}]$，以及相关数据 $Z \in \{0,1\}^n$，其中 $n \in [0, 2^{39}]$，返回密文 $C \in \{0,1\}^m$。

[0086] $H \leftarrow e(K, 0^w)$，$I \leftarrow e(K, 0^{w-1}||1)$，$J \leftarrow e(K, 0^{w-2}||10)$，$L \leftarrow e(K, 0^{w-2}||11)$

[0087] A ← P[0 ;w-1]

[0088] B ← P[w ;len(P)-1]

[0089] $C \leftarrow \mathbf{e}(K, A \oplus I)$

[0090] $D \leftarrow C \oplus \mathbf{h}(H, 0^w||Z, B)$

[0091] $E \leftarrow B \oplus \mathbf{c}(K, D, len(D))$

[0092] $F \leftarrow D \oplus \mathbf{h}(H, Z||L, E)$

[0093] $G \leftarrow \mathbf{d}(K, F) \oplus J$

[0094] 返回 G||E

[0095] 表 2-XCB 解密运算

[0096] 给出密钥 $K \in \{0,1\}^k$，密文 $C \in \{0,1\}^m$，其中 $m \in [w, 2^{39}]$，以及相关数据 $Z \in \{0,1\}^n$，其中 $n \in [0, 2^{39}]$，返回明文 $P \in \{0,1\}^m$。

[0097] $H \leftarrow e(K, 0^w)$，$I \leftarrow e(K, 0^{w-1}||1)$，$J \leftarrow e(K, 0^{w-2}||10)$，$L \leftarrow e(K, 0^{w-2}||11)$

[0098] G ← C[0 ;w-1]

[0099] E ← C[w ;len(C)-1]

[0100] $F \leftarrow \mathbf{e}(K, G \oplus J)$

[0101] $D \leftarrow F \oplus \mathbf{h}(H, Z||L, E)$

[0102] $B \leftarrow E \oplus \mathbf{c}(K, D, len(D))$

[0103] $C \leftarrow D \oplus \mathbf{h}(H, 0^w||Z, B)$

[0104] $A \leftarrow \mathbf{d}(K, C) \oplus I$

[0105] 返回 A||B

[0106] 函数 $c : \{0,1\}^k \times \{0,1\}^w \rightarrow \{0,1\}^l$，其中输出长度 l 由 0 <= l <= 2^{39} 限定，使用其 w 位输入作为初始计数器值，通过在计数器模式下运行块密码 e 而产生任意长度的输出。其定义为：

[0107] $C(K, W, l) = E(K, W)||E(K, incr(W))||...||MSB_t(E(K, incr^{n-1}(W)))$，

[0108] 其中为了清楚起见使输出长度 l 成为显性参数。表达式$n=\lceil l/w \rceil$是输出中 w 位的块的数目，t = l mod w 是尾块中的位数。此外，函数 incr :{0,1}^{w} → {0,1}^{w} 是用来产生连续的计数器值的递增运算。递增函数将其自变量的最右边 32 位当作非负整数，最低有效位在右边，并且以 2^{32} 为模递增该值。

[0109] 函数 h :{0,1}^{w} × {0,1}^{m} × {0,1}^{n} → {0,1}^{w}，m ∈ [w,2^{39}]，n ∈ [0,2^{39}] 是由 h(H,A,C) = X_{m+n+1} 定义的，其中变量 X_i ∈ {0,1}^{w}，对于 i = 0,...,m+n+1 被定义为：

[0110] X_i =

[0111] 0 对于 i = 0

[0112] $(X_{i-1} \oplus A_i) \cdot H$ 对于 i = 1,...,m-1

[0113] $(X_{m-1} \oplus (A^*_m \| 0^{w-v})) \cdot H$ 对于 i = m

[0114] $(X_{i-1} \oplus C_{i-m}) \cdot H$ 对于 i = m+1,...,m+n-1

[0115] $(X_{m+n-1}, \oplus (C^*_n \| 0^{w-u})) \cdot H$ 对于 i = m+n

[0116] $(X_{m+n}, \oplus (\mathrm{len}(A) \| \mathrm{len}(C))) \cdot H$ 对于 i = m+n+1

[0117] 在上述表达式中，A_i 表示 w 位的子串 A[(i-1)w :iw-1]，C_i 表示 C[(i-1)w :iw-i]。因此，如果那些位串被分解成 w 位的块，则 A_i 和 C_i 分别是 A 和 C 的第 i 块。在用作运算的 Galois/ 计数器模式 (GCM) 的组成部分的通用散列函数 GHASH 中提供类似的方法，除了 GHASH 像 AES 一样需要 w = 128。

[0118] 域 GF(2^{128}) 上的乘法被定义为关于位向量的运算以简化这里的详细说明。这样的定义不需要使用方法定义中的有限域数学。该域的背景信息和其表示法以及用于有效实现的策略在 GCM 规范 :D. McGrew 等人 2004 年 1 月的“The Galois/Counter Mode of Operation(GCM)”，Submission to NIST Modes of Operation Process 的第 3 和第 4 部分（在万维网上的域 csrc.nist.gov 的 CryptoToolkit/modes/proposed modes 目录中可在线得到）中提供。

[0119] 每个域元素是 128 位的向量。元素 X 的第 i 位表示为 X_i。最左边的位是 X_0，最右边的位是 X_{127}。乘法运算使用特定元素 R = 11100001||0^{120}，并且在表 3 中定义。函数 rightshift() 将其自变量的位右移一位。因此，任何时候 W = rightshift(V)，那么 W_i = V_{i-1} 对于 1 <= i <= 127 并且 W_0 = 0。

[0120] 表 3- 用于 GF(2^{128}) 的乘法

[0121] Z ← 0, V ← X

[0122] for i = 0to 127do

[0123] if Y_i = 1then

[0124] $Z \leftarrow Z \oplus V$

[0125] end if

[0126] if V_{127} = 0then

[0127] V ← rightshift(V)

[0128] else

[0129] $V \leftarrow \mathrm{rightshift}(V) \oplus R$

[0130] end if

[0131] end for

[0132] return Z

[0133] 3.3 示例应用

[0134] 示例实施例可以应用到数个不同的应用。图 3A 是示出安全电信系统的框图，图 3B 是示出安全存储管理系统的框图。现在参照图 3A，根据一个实施例，网络元件 304 包括实现图 1B 的方法的 XCB 逻辑 306，该网络元件被耦合到第一网络 305A 和第二网络 305B。第二网络元件 310 也被耦合到网络 305B。网络 305A 和 305B 可以包括相同的网络。

[0135] 网络元件 304 通过网络 305A 从上游网络元件（未示出）接收安全实时协议 (SRTP) 消息 302。消息 302 被认为是明文消息。网络元件 304 用 XCB 逻辑 306 对 SRTP 消息 302 应用这里所描述的运算的延伸代码块模式。所产生的密文被封装成加密的 SRTP 消息 308，加密的 SRTP 消息 308 与明文消息具有相同的长度或大小。然后网络元件 304 将加密的消息 308 转发给网络元件 310，网络元件 310 用这里的技术对该消息进行解密或者用其他方式使用该消息。这样，这里的技术可以被应用到任何网络通信情况中，其中特定的消息发送协议不能允许由于加密而产生的消息扩展。

[0136] 现在参照图 3B，存储管理元件 322 容宿或者实现 XCB 逻辑 306。存储管理元件 322 被耦合到大容量存储设备 330，例如盘阵列或盘驱动器。

[0137] 存储管理元件 322 从存储设备 330、操作系统、中央处理器或其他处理元件接收盘块 320 以便存储在存储设备 330 中。存储管理元件 322 用 XCB 逻辑 306 将这里所描述的运算的延伸代码块模式应用到盘块 320，从而创建加密的盘块 324。加密的盘块 324 具有与盘块 320 的长度或大小相同的长度或大小。然后存储管理元件 322 将加密的盘块 324 存储在存储设备 330 中。

[0138] 在所有这样的应用中，明文数据、段、中间结果数据、相关数据和密文中的每一项可以包括存储在电子数字存储设备中的数字值。此外，上面所描述的分开、加密、散列、XOR 和其他操作可以在耦合到电子数字存储设备并且与数字数据值交互的电子数字数据处理装置中执行。

[0139] 特定的应用可以在使用诸如安全 RTP 之类的协议的网络通信的环境中和在提供盘块的安全存储的存储管理等中实现。因此，这里的方法在技术领域内应用。

[0140] 这里的方法还提供有用的、具体的和真实的结果。在一个实施例中，所述方法接收可以作为瞬时电子信号而在计算机中表示出的数据值。在一个实施例中，所述方法使用电子数字数据处理器来根据这里所描述的数据处理步骤操纵信号。因此，输入明文被以特定方式变成输出密文。输出密文也被表示为可以存储在诸如数字存储器之类的电子数字设备中的瞬时电子信号。因此，这里所描述的机器实现的数据操纵步骤可以操作存储在电子计算机存储器中的数据；改变数据引起电子存储器的单元、门和晶体管的状态上的变化；改变这些器件的状态意味着在原子能级上，电子电荷被施加到与特定存储器位的位置相关联的某些半导体材料上并且不施加到其他材料上；并且电荷上的这种改变是具体和真实的结果。

[0141] 3.4 安全性证明

[0142] 可以证明这里的方法满足上面所确定的目标并且是安全的。这里的方法的安全性证明在 McGrew 等人的论文“Extended Codebook Mode(XCB):Security without Data

Expansion”（第 3 部分，“Security”）中给出，这篇论文在美国专利申请的附录中再现，本申请要求该美国专利申请的优先权。

[0143] 3.5 实施例的好处

[0144] 所公开的方法在其效率、其处理任意明文长度的能力和其接受另外输入的能力上是独特的。所述方法提供运算的块密码模式，该模式用另外的输入实现无展性密码。广泛地看，这里的方法从而明文数据通过三次以产生密文。两次通过使用 GF(2^{128}) 上的通用散列法，一次通过使用计数器模式加密。与所有基于 Luby-Rackoff 和 Naor-Reingold 的设计不同，这里的方法部分地依赖于块密码的可逆性来获得安全性。

[0145] 这里所公开的模式可以用硬件和软件实现，并且其具有与类似的模式相比相对低的计算成本：其仅需要 n+1 次块密码调用和 GF(2^w) 上的 2n 次乘法，其中 w 是块密码输入和输出中的位数。该模式还具有数个有用的属性：其接受任意大小的明文和相关数据，包括长度至少为 w 位的任何明文。该属性允许这里的模式保护短数据，例如安全 RTP 中的普通 20 字节 G.729 语音编解码器。

[0146] 3.6 与过去的方法的某些差别

[0147] XCB 比任何其他的无展性密码更高效，因为它需要较少的计算。仅次于最好模式的运算模式是 EME 模式，EME 模式几乎进行两倍的计算。此外，XCB 更适合于高效的硬件实现方式，因为它可以更容易地被并行化和流水线化。XCB 还接收另外的输入，该另外的输入可以用来防止密文置换攻击。

[0148] 这里的方法几乎是最好的竞争者效率的两倍。这里的方法在 AES 与伪随机排列不可区分的合理假设下也被证明为安全的。

[0149] 这里的方法具有很多应用。例如，该方法可以用在安全 RTP 中，其中它对于无线语音或者在 CET 中或者在分组或数据净荷的扩展不可行或不被协议允许的任何其他协议中尤其合适。

[0150] 该方法还可以用在存储联网中或者扩展不可行的数据存储系统中。该方法可以用在用于本地和远程存储两者的盘块加密中。

[0151] 4.0 实现机制 - 硬件概述

[0152] 图 4 是示出了本发明的实施例可以在上面实现的计算机系统 200 的框图。计算机系统 200 包括总线 202 或用于传送信息的其他通信机制以及与总线 202 耦合的用于处理信息的处理器 204。计算机系统 200 还包括诸如随机存取存储器（“RAM”）或其他动态存储设备之类的主存储器 206，主存储器 206 耦合到总线 202 并且用于存储信息和将由处理器 204 执行的指令。主存储器 206 也可以用于在执行将由处理器 204 执行的指令期间存储临时变量或其他中间信息。计算机系统 200 还包括耦合到总线 202 的只读存储器（“ROM”）208 或其他静态存储设备，用于存储用于处理器 204 的静态信息和指令。诸如磁盘或光盘之类的存储设备 210 被提供并且被耦合到总线 202，用于存储信息和指令。

[0153] 计算机系统 200 可以经由总线 202 耦合到显示器 212，显示器 212 例如是阴极射线管（“CRT”），用于将信息显示给计算机用户。包括字母数字键和其他键的输入设备 214 被耦合到总线 202，用于将信息和命令选择传送给处理器 204。另一类型的用户输入设备是光标控制设备 216，例如鼠标、跟踪球、触针或光标方向键，用于将方向信息和命令选择传送给处理器 204 并且用于控制光标在显示器 212 上的移动。该输入设备一般具有第一轴（例如

x）和第二轴（例如 y）两个轴上的两个自由度，允许设备在平面上指定位置。

[0154] 本发明涉及用于加密方法的计算机系统 200 的使用。根据本发明的一个实施例，响应于处理器 204 执行包含在主存储器 206 中的一个或多个指令的一个或多个序列而由计算机系统 200 提供加密方法。这样的指令可以从诸如存储设备 210 之类的另一计算机可读介质读入到主存储器 206 中。包含在主存储器 206 中的指令序列的执行从而处理器 204 执行这里所描述的处理步骤。在可替换的实施例中，可以使用硬连接的电路代替软件指令或者使用硬连接的电路与软件指令的组合来实现本发明。因此，本发明的实施例不局限于硬件电路和软件的具体组合。

[0155] 这里所使用的术语“计算机可读介质”指的是参与将指令提供给处理器 204 执行的任何介质。这样的介质可以采用多种形式，包括但不局限于非易失性介质、易失性介质和传输介质。非易失性介质例如包括光盘或磁盘，例如存储设备 210。易失性介质包括动态存储器，例如主存储器 206。传输介质包括同轴电缆、铜线和光纤，包括包含总线 202 的线路。传输介质也可以采用声波或光波的形式，例如在无线电波或红外数据通信期间产生的那些波。

[0156] 计算机可读介质的普通形式例如包括软盘、柔性盘、硬盘、磁带或任何其他磁介质，CD-ROM、任何其他光介质，穿孔卡、纸带、任何其他具有孔图案的物理介质，RAM、PROM 和 EPROM，FLASH-EPROM、任何其他存储器芯片或存储器盒 (memory cartridge)，下文所描述的载波或计算机可以对其读取的任何其他介质。

[0157] 在将一个或多个指令的一个或多个序列运载给处理器 204 执行的过程中可以涉及各种形式的计算机可读介质。例如，指令最初可以在远程计算机的磁盘上运载。远程计算机可以将指令载入到其动态存储器中并且用调制解调器在电话线上发送指令。计算机系统 200 本地的调制解调器可以接收电话线上的数据并且使用红外线发射器将数据转换为红外信号。红外检测器可以接收以红外信号运载的数据，适当的电路可以将数据放在总线 202 上。总线 202 将数据运载给主存储器 206，处理器 206 从主存储器 206 取回并执行指令。由主存储器 206 所接收的指令可以或者在处理器 204 执行之前，或者在处理器 204 执行之后被选择性地存储在存储设备 210 上。

[0158] 计算机系统 200 还包括耦合到总线 202 的通信接口 218。通信接口 218 提供耦合到网络链路 220 的双向数据通信，网络链路 220 被连接到本地网 222。例如，通信接口 218 可以是提供对相应类型的电话线的数据通信连接的综合业务数字网（“ISDN”）卡或调制解调器。作为另一示例，通信接口 218 可以是提供对兼容 LAN 的数据通信连接的局域网（“LAN”）卡。也可以实现无线链路。在任何这样的实现方式中，通信接口 218 发送和接收运载表示各种类型信息的数字数据流的电信号、电磁信号或光信号。

[0159] 网络链路 220 一般提供经过一个或多个网络到其他数据设备的数据通信。例如，网络链路 220 可以提供经过本地网 222 到主计算机 224 或到因特网服务提供商 (“ISP”) 226 操作的数据设备的连接。ISP 226 又提供经过现在一般称为“因特网”228 的全球分组数据通信网的数据通信服务。本地网 222 和因特网 228 都使用运载数字数据流的电信号、电磁信号或光信号。经过各种网络的信号和在网络链路 220 上并且经过通信接口 218 的信号将数字数据运载到计算机系统 200 或者从计算机系统 200 运载数字数据，它们是运输信息的载波的示例性形式。

[0160] 计算机系统 200 可以经过（一个或多个）网络、网络链路 220 和通信接口 218 发送消息并接收数据，包括程序代码。在因特网示例中，服务器 230 可以经过因特网 228、ISP 226、本地网 222 和通信接口 218 发送用于应用程序的请求代码。根据本发明，一个这样的下载应用为提供这里所描述的加密方法作准备。

[0161] 当代码被接收并且 / 或者被存储在存储设备 210 或其他非易失性存储设备以稍后执行时，处理器 204 可以执行所接收的代码。在这种方式下，计算机系统 200 可以获得载波形式下的应用代码。

[0162] 在上述具体描述中，参考本发明的具体实施例对本发明进行了描述。然而，将会清楚可以对其做出各种修改和变化，而不脱离本发明更宽的精神和范围。因此，说明书和附图被认为是说明性意义上的，而不是限制性意义上的。

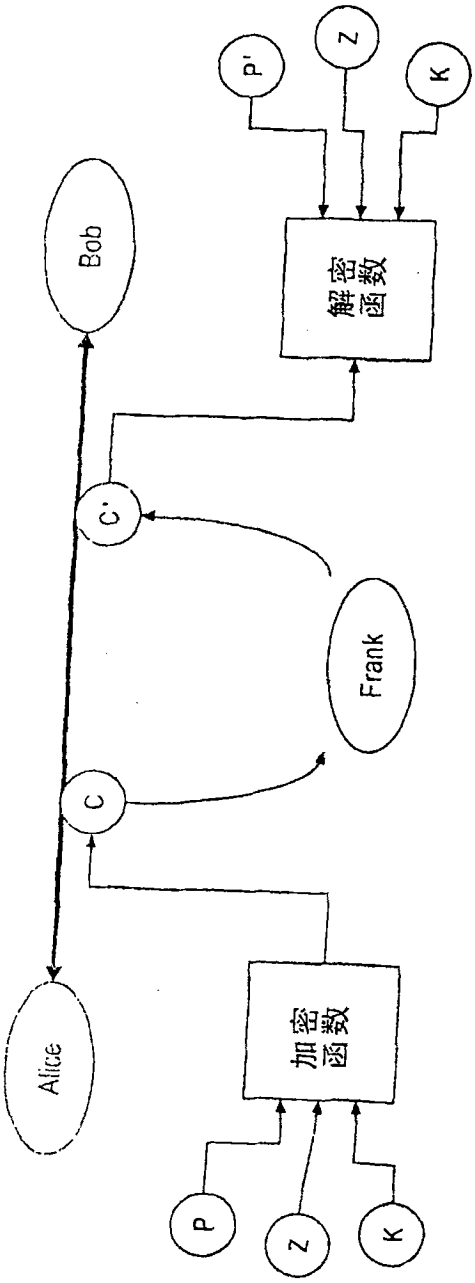


图 1A

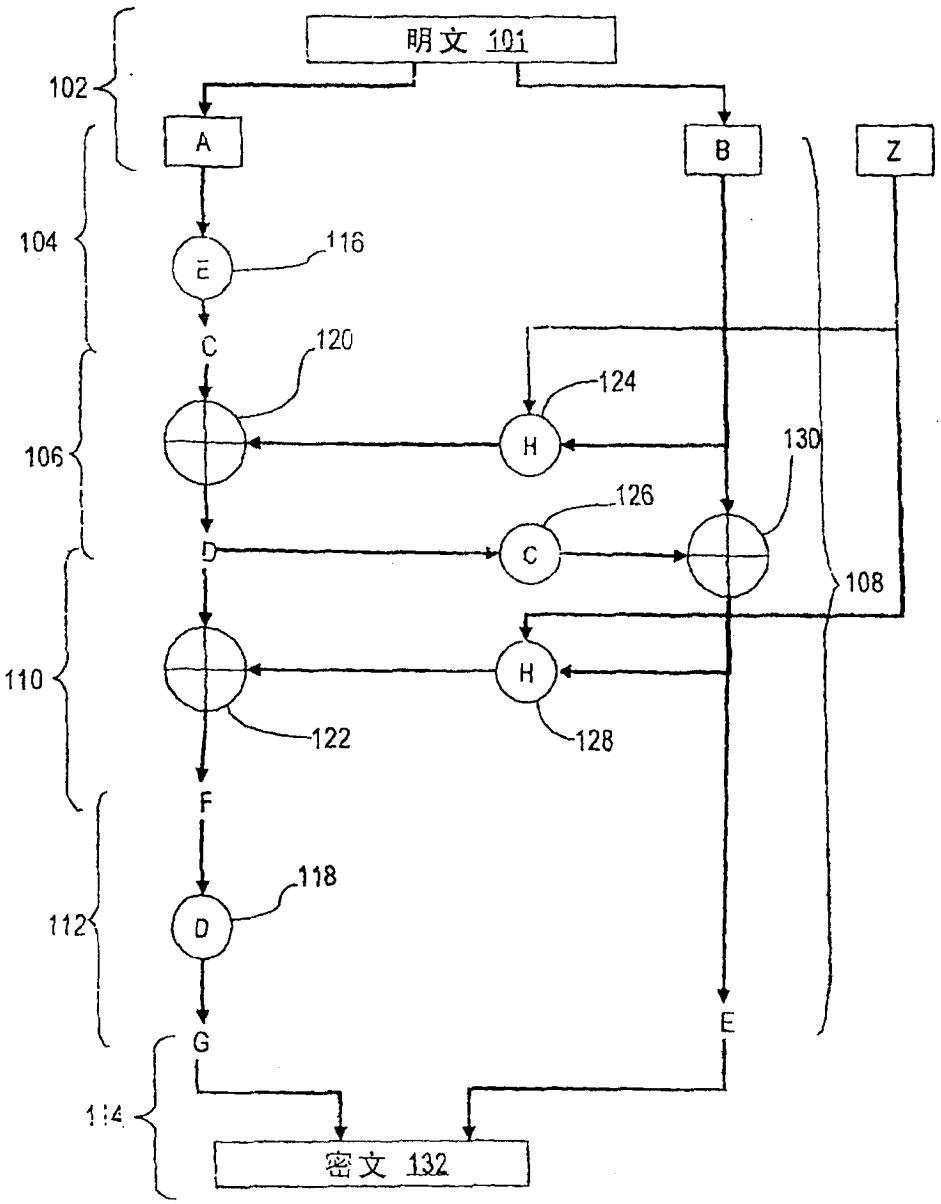

明文 101
102
A
B
Z
104
E
116
C
120
124
106
H
130
126
C
D
108
110
H
122
128
F
118
D
112
G
E
114
密文 132

图 1B

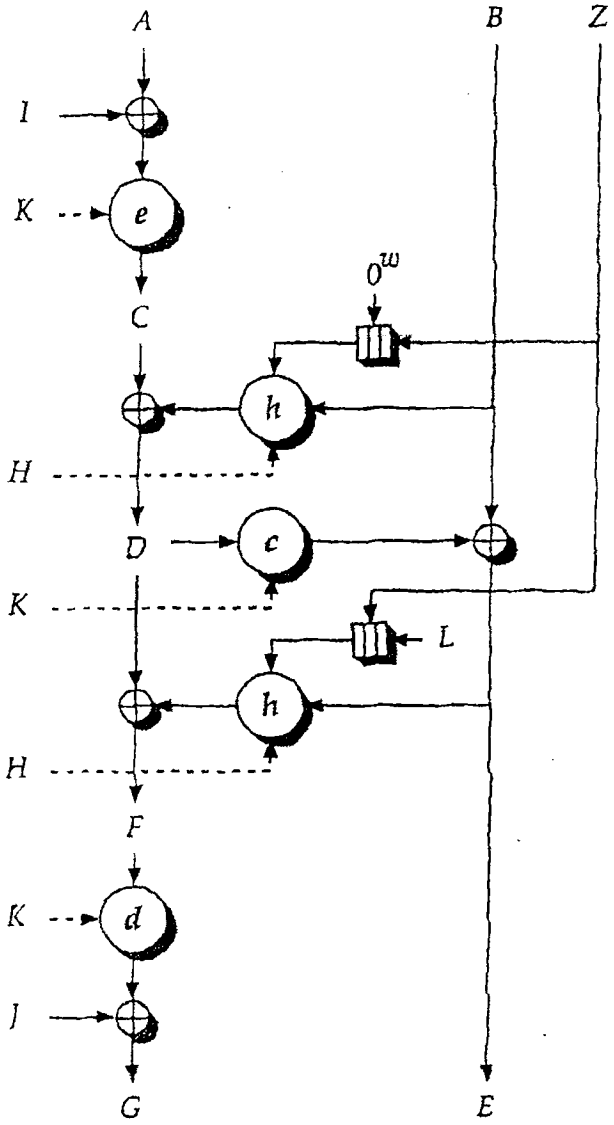


图 2A

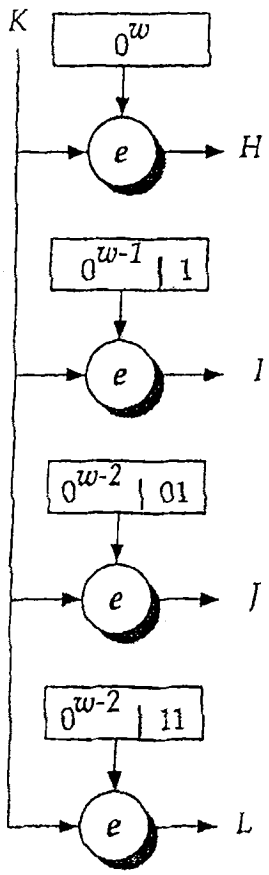


图 2B

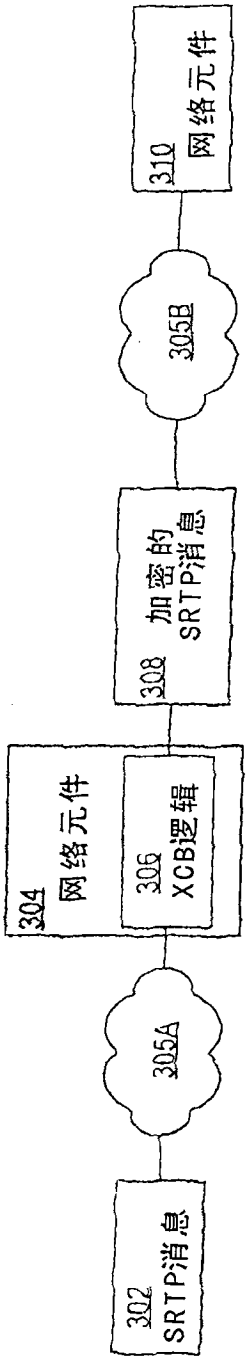

302
SRTP消息
305A
304
网络元件
306
XCB逻辑
308
加密的
SRTP消息
305B
310
网络元件

图 3A

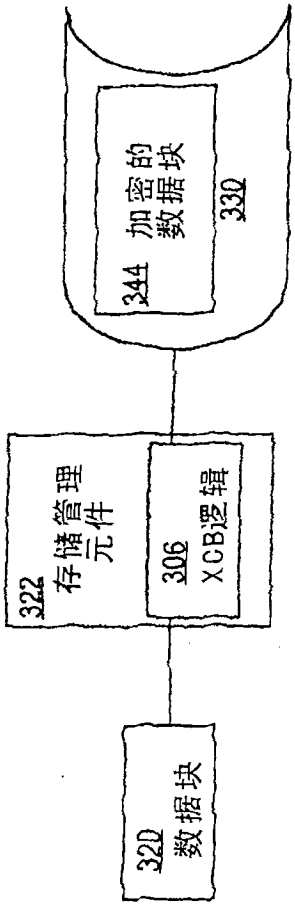

320
数据块
322
存储管理
元件
306
XCB逻辑
344
加密的
数据块
330

图 3B

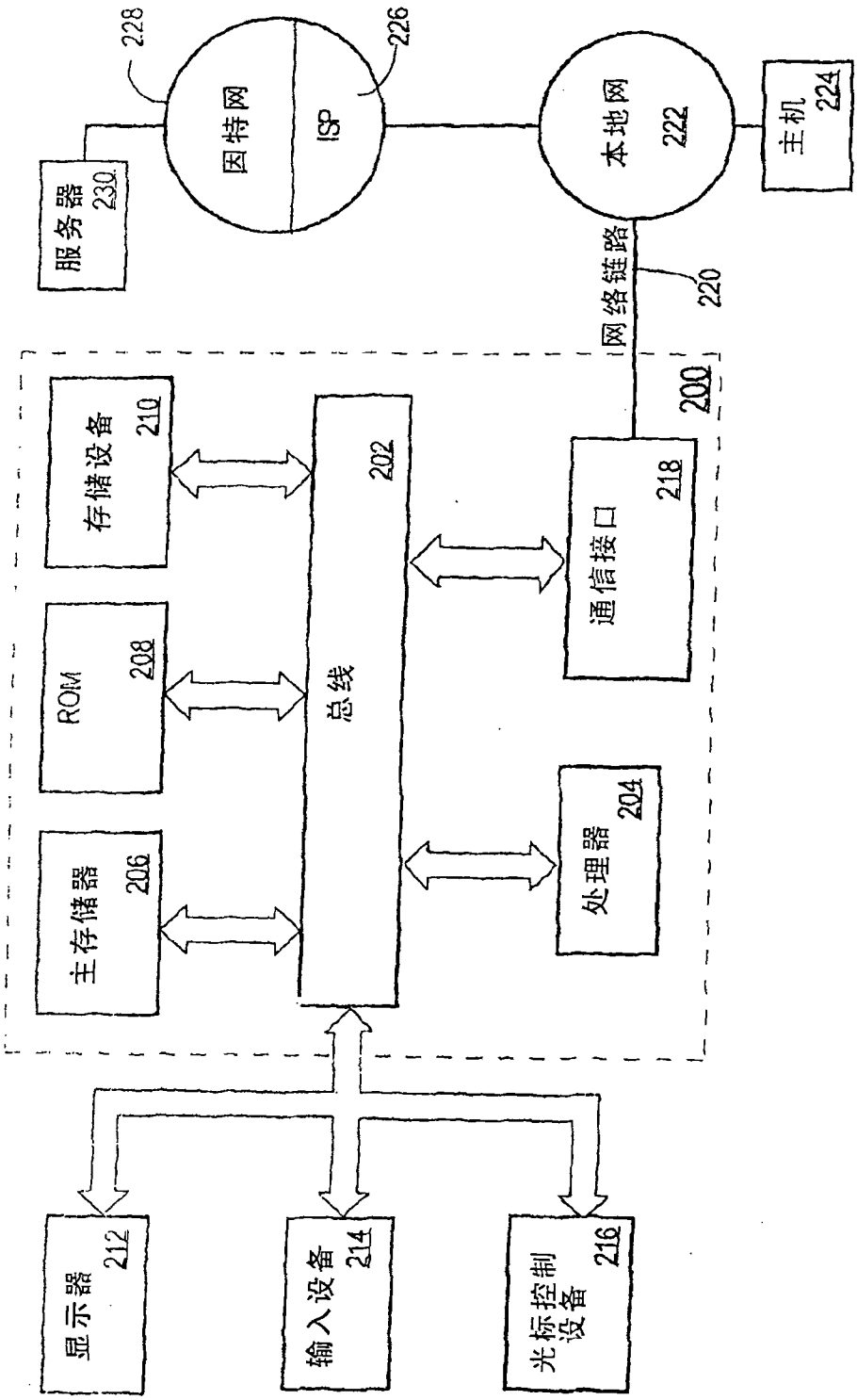

228
因特网
ISP
226
本地网
222
主机
224
服务器
230
网络链路
220
200
存储设备
210
202
通信接口
218
ROM
208
总线
主存储器
206
处理器
204
显示器
212
输入设备
214
光标控制设备
216

图 4