(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 102904717 B
(45)授权公告日 2015.06.03

(21)申请号 201210386406.9
(22)申请日 2012.10.13
(73)专利权人 华南理工大学
地址 510640 广东省广州市天河区五山路381号
(72)发明人 覃健诚 陆以勤
(74)专利代理机构 广州粤高专利商标代理有限公司 44102
代理人 何淑珍
(51)Int.Cl.
H04L 9/30(2006.01)
H04L 9/08(2006.01)
H04L 9/00(2006.01)

(56)对比文件
包先雨,蒋建国,李援. 一种适合于H.264实时视频传输的新型加密方案.《电子学报》.2006,第34卷(第11期),引言,第3节,第5节.

审查员 常志沛

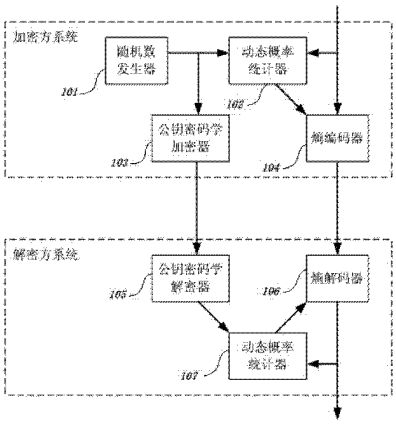
权利要求书2页 说明书8页 附图4页

(54)发明名称

利用数据压缩编码的混沌同步加密解密方法及其装置

(57)摘要

本发明公开利用数据压缩编码的混沌同步加密解密方法及其装置,该装置包括随机数发生器、公钥密码学加密器、公钥密码学解密器、动态概率统计器、熵编码器和熵解码器。该方法是:把数据压缩用的熵编码器、动态概率统计器作为混沌动力学系统,使压缩编码过程成为混沌密码学加密过程;把公钥密码学加密器与混沌动力学系统相结合,发送方用非对称加密方法来加密随机生成的会话密钥之后,传送给接收方;发送、接收双方各自用会话密钥来初始化自己的混沌动力学系统,使双方的系统状态同步;发送方用初始化之后的系统进行数据压缩编码,接收方以状态保持一致的系统进行数据解压缩。本发明支持超长密钥,提高加密安全性,同时加密速度不受密钥长度影响。



CN 102904717 B

1.一种利用数据压缩编码的混沌同步加密解密方法，其特征在于，该方法包括如下步骤：

（1）把数据压缩用的熵编码器、动态概率统计器作为混沌动力学系统，使压缩编码过程成为混沌密码学加密过程；具体包括：

熵编码器采用任意的压缩编码算法，根据字符出现的概率来确定字符编码的长短，字符出现的概率信息取自动态概率统计器；

动态概率统计器以一张或多张统计表的形式，统计每个字符在各种情况下出现的次数，并能根据统计表来预测下一个将要出现的是哪个字符的概率；

熵编码器、动态概率统计器均为有限状态自动机，由熵编码器的状态与动态概率统计器的状态共同组成混沌动力学系统的状态，每当加解密双方编码或解码一个字符，各自的系统状态就根据这个字符的不同而作相应变化，双方状态保持同步，才能使编码的字符与解码出来的字符相同；

（2）把公钥密码学加密器与混沌动力学系统相结合，加密方用非对称加密方法来加密随机生成的会话密钥之后，传送给解密方；具体包括：

公钥密码学加密器采用任意的非对称加密算法或者密钥交换算法，每次进行混沌同步加密之前，先由加密方生成长度为N位的随机二进制数K作为会话密钥，N是自然数；

加密方用公钥密码学加密器对会话密钥K进行加密后，传送给解密方，解密方用相应的解密器还原出会话密钥K；

（3）加解密双方各自用会话密钥来初始化自己的混沌动力学系统，使双方的系统状态同步；具体包括：

加密方直接把会话密钥K当作字符串，送入熵编码器中进行压缩编码，从而使混沌动力学系统的状态根据的具体数据而发生变化；

加密方把会话密钥K压缩之后的二进制编码数据直接丢弃，不传送给解密方；

解密方直接进行虚拟的解压缩，在解码器中模拟解压会话密钥K的情形，从而使混沌动力学系统的状态根据K的具体数据而发生变化，与发送方的系统状态保持一致；

（4）加密方用初始化之后的系统进行常规的数据压缩编码，解密方以状态保持一致的系统进行常规的数据解压缩。

2.根据权利要求1所述的利用数据压缩编码的混沌同步加密解密方法，其特征在于，步骤（4）具体包括：

加密方在直接加密会话密钥K并丢弃压缩后的二进制编码数据之后，用熵编码器以常规的压缩方式对真正的明文字符串M进行压缩，压缩后的二进制编码数据E作为密文传送给解密方；

解密方在模拟解压会话密钥K使系统状态与发送方保持一致之后，对来自加密方的密文E以常规的解压方式进行解压缩，解出来的字符串就是明文M。

3.用于实现权利要求1所述利用数据压缩编码的混沌同步加密解密方法的装置，其特征在于包括：

随机数发生器，用于生成随机的会话密钥K，提供给公钥密码学加密器；

公钥密码学加密器，用于加密会话密钥K，发送给解密方；

公钥密码学解密器，用于解密会话密钥K；

动态概率统计器，用于实时统计压缩或解压过程中各种字符在不同情况下出现的次数，并且向熵编码器或熵解码器提供下一个将要出现的是哪个字符的概率信息；

熵编码器，用于以常规的压缩方式，根据字符出现的概率来确定字符编码的长短，把会话密钥 K 和真正的明文 M 进行压缩编码；

熵解码器，用于以常规的解压方式，虚拟解压会话密钥 K，以及实际解压真正的明文 M；

所述随机数发生器包括电子电流计的传感器、运算放大器和 A/D 转换电路；

所述公钥密码学加密器、公钥密码学解密器，均包括单片机或 FPGA 逻辑电路；

所述动态概率统计器包括存储器和单片机或 FPGA 逻辑电路；

所述熵编码器包括单片机或 FPGA 逻辑电路；

由所述随机数发生器、公钥密码学加密器、动态概率统计器、熵编码器组成加密方系统；由所述公钥密码学解密器、动态概率统计器、熵解码器组成解密方系统；加密方系统、解密方系统均为混沌动力学系统，加密方系统、解密方系统之间的连接方式为有线网络、无线网络、串行总线或并行总线连接。

利用数据压缩编码的混沌同步加密解密方法及其装置

技术领域

[0001] 本发明涉及数据加密解密编码的信息安全技术，特别涉及一种利用数据压缩进行加密解密的方法及装置。

背景技术

[0002] 21 世纪是信息化的时代，信息安全关系到国计民生，而信息编码又是信息安全的基础性技术。信息编码技术领域有三大核心 :1、信源编码，主要对应数据压缩 ;2、保密编码，主要对应数据加密 ;3、信道编码，主要对应数据纠错编码。本发明涉及数据压缩和加密技术，并且与混沌密码学、公钥密码学和无损压缩的熵编码知识相关。

[0003] 混沌密码学是把物理学中的混沌动力学与信息学中的现代密码学相结合，基本做法是利用混沌动力学系统(简称混沌系统)的“蝴蝶效应”特性，即混沌系统本身的变化是确定的、有规律可循的，但是对初始状态非常敏感，稍微一点状态改变就会引起整个系统状态的巨大变化，从而导致宏观上对系统的状态变化不可预知。混沌系统的这种特性可以用来生成超长、不重复的数据流密码 C，以某种可逆算法(例如异或、相加等)把这种流密码 C 与明文 M 相结合成为密文 E，就完成了加密的过程。解密则是采用逆运算把明文 M 解出来，这就需要有加密时所用到的流密码 C。

[0004] 加密时，用密钥 K 来影响混沌系统的初始状态，就能得到相应的流密码 C。解密时，采用同步的混沌系统状态，就能得到相同的流密码 C，而使混沌系统状态与加密时的状态同步的关键就在于有密钥 K 可以使初始状态相同。

[0005] 公钥密码学是相当成熟的加密理论和技术，例如 RSA、Elgamal、椭圆曲线等加密算法就是现在常见的公钥密码学算法。单密钥加密系统如 DES、AES 等算法的系统在加密、解密时采用同一个密钥，而公钥密码学的系统则采用一对密钥——公钥和私钥，加密时采用其中一个密钥，解密时用另一个。

[0006] 公钥密码学中还有一种密钥交换算法，例如 DHM 算法(以前称为 Diffie-Hellman 算法)，本身并没有一对公钥、私钥来进行明文的加密和解密，而仅仅是双方共同协商出一个随机的会话密钥。本发明所涉及到的公钥密码学加密器、解密器对上述情况同样适用。

[0007] 无损压缩又称为无失真压缩，是数据压缩技术之中的一类，特点是解压缩时能够把数据一模一样地还原出来。例如 WinZip、WinRAR、7-zip 等软件采用的就是无损压缩技术。数据压缩技术的另一类称为有损压缩，通常压缩的对象是声音、图片、视频等多媒体数据，其特点是解压缩得到的数据与原始数据有差异，但是给人的感觉差距不明显。例如 JPG 图片、DVD 视频就用到了有损压缩技术。所有的有损压缩编码方法，都需要在压缩系统末端采用一个无损压缩的编码部件来完成压缩，因此本发明对于有损压缩的情况同样适用。

[0008] 熵编码器是无损压缩技术中的重要部件，其原理是根据字符出现的概率来确定字符编码的长短，概率大的字符采用短编码，概率小的字符采用长编码，从而使输出的数据编码尽可能短，达到数据压缩的效果。熵编码器采用的常见算法有算术编码、区间编码、Huffman 编码等，例如 WinZip 用了 Huffman 编码，7-zip 用了区间编码的算法。本发明对于

采用了其他压缩编码算法，如 LZ 系列算法的情况同样适用。

[0009] 本发明所指的“字符”是抽象概念，不仅限于字母、数字符号，而要根据实际算法的不同，成串的符号组合、数据字典索引和其他数据结构都可以视为字符。

[0010] 密钥长度对于加密系统的安全性有重要影响，但加密系统本身也必须没有漏洞，不会被攻击者绕过加密保护。现有的数据加密技术主要包括：1、单密钥加密技术；2、公钥加密技术；3、公钥与单密钥加密相结合的技术；4、混沌系统生成流密码再进行加密的技术。简单介绍如下：

[0011] 现有技术一：单密钥加密技术。

[0012] 原理：加密和解密采用同样的密钥 K，使用可逆算法对明文 M 进行加密。解密时采用逆运算还原出明文 M。

[0013] 优点：与公钥加密技术相比，同样的密钥长度下运算速度比较高，加密强度比较大。

[0014] 缺点：密钥 K 如何安全地分发、传送给解密方是个难题，多方之间两两使用不同的密钥进行加密和解密时，密钥的管理和安全保护也会成为难题。加密速度通常会随着密钥长度的增长而下降，因此密钥 K 无法做到很长而又不影响性能。

[0015] 现有技术二：公钥加密技术。

[0016] 原理：采用一对密钥——公钥和私钥，用其中一个密钥来加密，用另一个来解密。加密的安全性由数学上的各种单向函数的算法来保障。

[0017] 优点：公钥可以对外公开，只要保护好私钥即可保障加密的安全性。从而解决了密钥管理和安全分发、传送的难题。

[0018] 缺点：与单密钥加密技术相比，同样的密钥长度下运算速度比较慢，加密强度比较低。加密速度也会随着密钥长度的增长而下降，因此密钥 K 无法做到很长而又不影响性能。

[0019] 现有技术三：公钥与单密钥加密相结合的技术。

[0020] 原理：公钥加密技术用于安全传送单密钥加密所用的密钥 K，而单密钥加密技术用于对真正的明文 M 加密。每次加密时，先由加密方随机生成一个会话密钥 K，用公钥加密技术对密钥 K 加密之后传送给解密方，解密方解出密钥 K。然后双方都使用会话密钥 K，以单密钥加密的方式对真正的明文 M 进行加密和解密。

[0021] 优点：既有单密钥加密技术的速度快、加密强度高的优点，又有公钥加密技术的密钥容易管理，会话密钥分发、传送的安全性好的优点。

[0022] 缺点：加密速度仍然会随着密钥长度的增长而下降，因此密钥 K 同样无法做到很长而又不影响性能。

[0023] 现有技术四：混沌系统生成流密码再进行加密的技术。

[0024] 原理：利用混沌系统对初始条件敏感和状态演化的不可预测特性，使用密钥 K 来扰动系统的初始状态之后，让系统自动生成超长、不重复的数据流密码 C。加密时以某种可逆算法(例如异或、相加等)把这种流密码 C 与明文 M 相结合成为密文 E，解密时采用逆运算把明文 M 解出来。

[0025] 优点：流密码 C 的生成取决于密钥 K，密钥 K 只是在混沌系统状态初始化的时候参与运算，因此密钥 K 可以很长，并且密钥 K 的长度对真正的加密过程性能没有影响。

[0026] 缺点：仍然属于单密钥加密技术，因此也存在密钥管理和安全分发、传送的难题。

而且需要专门使用混沌系统来生成流密码 C，提高加密成本。而加密运算即使如异或、相加那么简单，也是需要为加密而消耗计算资源。

[0027] 综上所述，现有的数据加密技术要么速度慢，要么密钥长度会影响加密性能，无法实现超长的密钥，要么需要专门的系统来生成流密码，而且加密过程仍然需要消耗计算资源。

[0028] “超长密钥”是个相对概念，以目前的技术水平，二进制 4000 位以上的密钥可以视为超长密钥，且没有长度上限。随着技术的发展，超长密钥的长度下限可能会加长。

发明内容

[0029] 本发明的目的在于克服现有技术存在的上述不足，提供一种利用数据压缩编码的混沌同步加密解密方法及其装置，把混沌系统加密直接利用数据压缩来实现，无须专门的加密明文的过程，具体技术方案如下。

[0030] 一种利用数据压缩编码的混沌同步加密解密方法，该方法包括如下步骤：

[0031] （1）把数据压缩用的熵编码器、动态概率统计器作为混沌动力学系统，使压缩编码过程成为混沌密码学加密过程；

[0032] （2）把公钥密码学加密器与混沌动力学系统相结合，加密方用非对称加密方法来加密随机生成的会话密钥之后，传送给解密方；

[0033] （3）加解密双方各自用会话密钥来初始化自己的混沌动力学系统，使双方的系统状态同步；

[0034] （4）加密方用初始化之后的系统进行常规的数据压缩编码，解密方以状态保持一致的系统进行常规的数据解压缩。

[0035] 进一步优化的，步骤（1）具体包括：

[0036] 熵编码器采用任意的压缩编码算法，根据字符出现的概率来确定字符编码的长短，字符出现的概率信息取自动态概率统计器；

[0037] 动态概率统计器以一张或多张统计表的形式，统计每个字符在各种情况下出现的次数，并能根据统计表来预测下一个将要出现的是哪个字符的概率；

[0038] 熵编码器、动态概率统计器均为有限状态自动机，由熵编码器的状态与动态概率统计器的状态共同组成混沌动力学系统的状态，每当加解密双方编码或解码一个字符，各自的系统状态就根据这个字符的不同而作相应变化，双方状态保持同步，才能使编码的字符与解码出来的字符相同。

[0039] 进一步优化的，步骤（2）具体包括：

[0040] 公钥密码学加密器采用任意的非对称加密算法或者密钥交换算法，每次进行混沌同步加密之前，先由加密方生成长度为 N 位的随机二进制数 K 作为会话密钥，N 是自然数；

[0041] 加密方用公钥密码学加密器对会话密钥 K 进行加密后，传送给解密方，解密方用相应的解密器还原出会话密钥 K。

[0042] 进一步优化的，步骤（3）具体包括：

[0043] 加密方直接把会话密钥 K 当作字符串，送入熵编码器中进行压缩编码，从而使混沌动力学系统的状态根据的具体数据而发生变化；

[0044] 加密方把会话密钥 K 压缩之后的二进制编码数据直接丢弃，不传送给解密方；

[0045] 解密方直接进行虚拟的解压缩，在解码器中模拟解压会话密钥 K 的情形，从而使混沌动力学系统的状态根据 K 的具体数据而发生变化，与发送方的系统状态保持一致；

[0046] 进一步优化的，步骤（4）具体包括：

[0047] 加密方在直接加密会话密钥 K 并丢弃压缩后的二进制编码数据之后，用熵编码器以常规的压缩方式对真正的明文字符串 M 进行压缩，压缩后的二进制编码数据 E 作为密文传送给解密方；

[0048] 解密方在模拟解压会话密钥 K 使系统状态与发送方保持一致之后，对来自加密方的密文 E 以常规的解压方式进行解压缩，解出来的字符串就是明文 M。

[0049] 用于实现所述利用数据压缩编码的混沌同步加密解密方法的装置，该装置包括：

[0050] 随机数发生器，用于生成随机的会话密钥 K，提供给公钥密码学加密器；

[0051] 公钥密码学加密器，用于加密会话密钥 K，发送给解密方；

[0052] 公钥密码学解密器，用于解密会话密钥 K；

[0053] 动态概率统计器，用于实时统计压缩或解压过程中各种字符在不同情况下出现的次数，并且向熵编码器或熵解码器提供下一个将要出现的是哪个字符的概率信息；

[0054] 熵编码器，用于以常规的压缩方式，根据字符出现的概率来确定字符编码的长短，把会话密钥 K 和真正的明文 M 进行压缩编码；

[0055] 熵解码器，用于以常规的解压方式，虚拟解压会话密钥 K，以及实际解压真正的明文 M。

[0056] 进一步优化的，所述随机数发生器可以包括电子电流计的传感器、运算放大器和 A/D 转换电路；

[0057] 所述公钥密码学加密器、公钥密码学解密器，均可以包括单片机或 FPGA 逻辑电路；

[0058] 所述动态概率统计器可以包括存储器和单片机或 FPGA 逻辑电路；

[0059] 所述熵编码器可以包括单片机或 FPGA 逻辑电路；

[0060] 由所述随机数发生器、公钥密码学加密器、动态概率统计器、熵编码器组成加密方系统；由所述公钥密码学解密器、动态概率统计器、熵解码器组成解密方系统；加密方系统、解密方系统均为混沌动力学系统，加密方系统、解密方系统之间的连接方式为有线网络、无线网络、串行总线或并行总线连接。

[0061] 与现有技术相比，本发明具有如下优点和技术效果：本发明解决了现有加密技术存在的几个问题：1、密钥长度会影响加密性能，无法实际应用超长密钥；2、超长密钥的管理和安全分发、传送存在困难；3、如果使用混沌加密来解决密钥问题，则需要专门的混沌系统来生成流密码，而且加密过程仍然需要消耗计算资源。

[0062] 本发明把数据压缩用的熵编码器、动态概率统计器作为混沌动力学系统，使压缩编码过程成为混沌密码学加密过程；把公钥密码学加密器与混沌动力学系统相结合，发送方用非对称加密方法来加密随机生成的会话密钥之后，传送给接收方；发送、接收双方各自用会话密钥来初始化自己的混沌动力学系统，使双方的系统状态同步；发送方用初始化之后的系统进行常规的数据压缩编码，接收方以状态保持一致的系统进行常规的数据解压缩，从而达到了支持超长密钥，提高加密安全性，同时加密速度不受密钥长度影响的效果。

[0063] 本发明的熵编码器采用类似于算术编码的自适应区间编码压缩算法，动态概率统

计器采用 PPM (Prediction by Partial Match,部分匹配预测)算法,公钥密码学加密器采用 RSA 加密算法,会话密钥采用 4000 位以上的超长密钥。

附图说明

[0064] 图 1 为本发明实施例提供的一种利用数据压缩编码的混沌同步加密和解密装置结构示意图;

[0065] 图 2 为本发明实施例利用数据压缩编码的混沌同步加密方法流程图;

[0066] 图 3 为本发明实施例利用数据压缩编码的混沌同步解密方法流程图;

[0067] 图 4 为本发明实施例数据压缩编码的混沌同步加密和解密装置的连接关系示意图。

具体实施方式

[0068] 以下内容仅为举例,不用于限制本发明的保护范围。

[0069] 针对现有加密技术的密钥长度会影响加密性能,导致超长密钥难以实际应用的问题,本实施例把数据压缩用的自适应区间编码器、PPM 算法动态概率统计器作为混沌动力学系统,使压缩编码过程成为混沌密码学加密过程;把公钥密码学加密器与混沌动力学系统相结合,发送方用 RSA 公钥密码算法来加密随机生成的会话密钥之后,传送给接收方;发送、接收双方各自用会话密钥来初始化自己的混沌动力学系统,使双方的系统状态同步;发送方用初始化之后的系统进行常规的数据压缩编码,接收方以状态保持一致的系统进行常规的数据解压缩,从而达到了支持超长密钥,提高加密安全性,同时加密速度不受密钥长度影响的效果,解决了上述问题。

[0070] 如图 1 所示,本实施例提供的一种利用数据压缩编码的混沌同步加密和解密装置包括:

[0071] 随机数发生器 101,用于生成随机的会话密钥 K,提供给公钥密码学加密器 103;

[0072] 动态概率统计器 102,用于实时统计压缩过程中各种字符在不同情况下出现的次数,并且向熵编码器 104 提供下一个将要出现的是哪个字符的概率信息;

[0073] 公钥密码学加密器 103,用于加密会话密钥 K,发送给解密方;

[0074] 熵编码器 104,用于以某种压缩编码算法,根据字符出现的概率来确定字符编码的长短,把会话密钥 K 和真正的明文 M 进行压缩编码;

[0075] 公钥密码学解密器 105,用于解密会话密钥 K;

[0076] 熵解码器 106,用于以相应的解压算法,虚拟解压会话密钥 K,以及实际解压真正的明文 M;

[0077] 动态概率统计器 107,用于实时统计解压过程中各种字符在不同情况下出现的次数,并且向熵解码器 106 提供下一个将要出现的是哪个字符的概率信息;

[0078] 由随机数发生器 101、公钥密码学加密器 103、动态概率统计器 102、熵编码器 104 构成的加密方系统是混沌动力学系统,由公钥密码学解密器 105、动态概率统计器 107、熵解码器 106 构成的解密方系统也是混沌动力学系统,这两个混沌动力学系统的状态需要保持同步,才能够正确地进行数据压缩和解压。

[0079] 如图 2 所示,本实施例提供的一种利用数据压缩编码的混沌同步加密方法流程包

括下列步骤：

[0080] S201：用随机数发生器 101 生成随机的 N 位会话密钥 K。

[0081] S202：用公钥密码学加密器 101 以 RSA 算法，用公钥 K1 对 K 进行加密，生成密文 E0。

[0082] S203：把密文 E0 发送给解密方。

[0083] S204：初始化动态概率统计器 102，把所有字符统计表的计数值清零。

[0084] S205：用字符串数组 S 来保存会话密钥 K，变量 L 保存字符串长度。

[0085] S206：循环变量 i 从 0 开始。

[0086] S207：根据下标 i，取字符串数组 S 的一个字符，放在变量 M0 中。

[0087] S208：用熵编码器 104 以自适应区间编码算法对 M0 进行压缩编码，但压缩得到的二进制数据流不输出，直接丢弃。

[0088] S209：动态概率统计器 102 更新字符统计表中字符 M0 的计数值。

[0089] S210：循环变量 i 加 1。

[0090] S211：如果 i<L，则字符串 S 还没有处理完，转到 S207；否则跳出循环，转到 S212。

[0091] S212：读取真正要加密的明文的下一个字符，放在变量 M 中。

[0092] S213：如果已经没有要加密的字符，则结束加密流程；否则转到 S214。

[0093] S214：用熵编码器 104 对 M 进行压缩编码，压缩得到的二进制数据流也就是加密数据流，放在变量 E 中。

[0094] S215：把当前得到的数据流 E 发送给解密方。

[0095] S216：动态概率统计器 102 更新字符统计表中字符 M 的计数值，并转到 S212。

[0096] 如图 3 所示，本实施例提供的一种利用数据压缩编码的混沌同步解密方法流程包括下列步骤：

[0097] S301：从加密方获取密文 E0。

[0098] S302：用公钥密码学解密器 105 以 RSA 算法，用私钥 K2 对 E0 进行解密，得到会话密钥 K。

[0099] S303：初始化动态概率统计器 107，把所有字符统计表的计数值清零。

[0100] S304：用字符串数组 S 来保存会话密钥 K，变量 L 保存字符串长度。

[0101] S305：循环变量 i 从 0 开始。

[0102] S306：根据下标 i，取字符串数组 S 的一个字符，放在变量 M0 中。

[0103] S307：用熵解码器 106 以自适应区间编码算法对 M0 进行虚拟压缩编码，而压缩得到的二进制数据流不输出，直接丢弃。

[0104] S308：动态概率统计器 107 更新字符统计表中字符 M0 的计数值。

[0105] S309：循环变量 i 加 1。

[0106] S310：如果 i<L，则字符串 S 还没有处理完，转到 S306；否则跳出循环，转到 S311。

[0107] S311：从加密方获取加密数据流 E 的一段。

[0108] S312：如果数据流 E 已经结束，则结束解密流程；否则转到 S313。

[0109] S313：用熵解码器 106 对数据流 E 进行解压，获得的字符放在变量 M 中。

[0110] S314：向接收者输出解压之后的字符 M。

[0111] S315：动态概率统计器 107 更新字符统计表中字符 M 的计数值，并转到 S311。

[0112] 对本领域技术人员来说本实例中个部分的实现可以但不限于如下器件实现，例如，所述随机数发生器，可以由高灵敏度电子电流计的传感器、运算放大器、A/D 转换电路组成，用于实时检测流过本发明装置的电流大小，放大之后取其最低 4 位数值，多次取样拼接后作为随机数；所述公钥密码学加密器、公钥密码学解密器，可以由单片机（或 FPGA 逻辑电路）构成，其运算功能来自于单片机程序（或逻辑电路的设计）；所述动态概率统计器，可以由 DRAM（或 SRAM）存储器、单片机（或 FPGA 逻辑电路）组成，其运算功能来自于单片机程序（或逻辑电路的设计）；所述熵编码器，可以由单片机（或 FPGA 逻辑电路）构成，其运算功能来自于单片机程序（或逻辑电路的设计）。由随机数发生器、公钥密码学加密器、动态概率统计器、熵编码器组成加密方系统，加密方系统的各组成部分之间通过串行（或并行）总线连接，总线能够双向传输指令信号和数据；由公钥密码学解密器、动态概率统计器、熵解码器组成解密方系统，解密方系统的各组成部分之间通过串行（或并行）总线连接，总线能够双向传输指令信号和数据；加密方系统、解密方系统均为混沌动力学系统，这两个混沌动力学系统的状态需要保持同步，才能够正确地进行数据压缩和解压，这两个系统之间的连接是如下方式之一：有线网络、无线网络、串行总线、并行总线。

[0113] 如图 4 所示，本实施例提供的数据压缩编码的混沌同步加密和解密装置的连接关系包括：

[0114] 总线 A401 连接动态概率统计器 102、熵编码器 104、系统对外界的数据端口。总线 A401 所传输的信息包括：1、明文数据流，从数据端口传至动态概率统计器 102、熵编码器 104；2、数据接收响应信号，从熵编码器 104 传至数据端口。

[0115] 总线 B402 连接随机数发生器 101、动态概率统计器 102、公钥密码学加密器 103。总线 B402 所传输的信息包括：1、随机数比特流，从随机数发生器 101 传至公钥密码学加密器 103、动态概率统计器 102；2、会话密钥 K，从公钥密码学加密器 103 传至动态概率统计器 102。

[0116] 总线 C403 连接动态概率统计器 102、熵编码器 104。总线 C403 所传输的信息包括：1、待编码字符序号，从熵编码器 104 传至动态概率统计器 102；2、字符概率预测值相关数据，从动态概率统计器 102 传至熵编码器 104；3、字符统计值更新信号，从熵编码器 104 传至动态概率统计器 102。

[0117] 总线 D404 连接公钥密码学加密器 103、熵编码器 104、网络或总线 E 与总线 D 的接口。总线 D404 所传输的信息包括：1、密钥交换相关加密数据，在公钥密码学加密器 103 与总线 D － E 接口之间双向传输；2、会话密钥 K，从公钥密码学加密器 103 传至熵编码器 104；3、密文数据流，从熵编码器 104 传至总线 D － E 接口；4、同步控制信号，在熵编码器 104 与总线 D － E 接口之间双向传输。

[0118] 网络或总线 E405，连接加密方系统的总线 D、解密方系统的总线 F。网络或总线 E 所传输的信息包括：1、密钥交换相关加密数据，在总线 D － E 接口、总线 E － F 接口之间双向传输；2、密文数据流，总线 D － E 接口传至总线 E － F 接口；3、同步控制信号，在总线 D － E 接口、总线 E － F 接口之间双向传输。

[0119] 总线 F406，连接公钥密码学解密器 105、熵解码器 106、网络或总线 E 与总线 F 的接口。总线 F 所传输的信息包括：1、密钥交换相关加密数据，在公钥密码学解密器 105 与总线 E － F 接口之间双向传输；2、会话密钥 K，从公钥密码学解密器 105 传至熵解码器 106；3、密

文数据流，从总线 E — F 接口传至熵解码器 106；4、同步控制信号，在熵解码器 106 与总线 E — F 接口之间双向传输。

[0120] 总线 G407 连接公钥密码学解密器 105、动态概率统计器 107。总线 G 所传输的信息包括：会话密钥 K，从公钥密码学解密器 105 传至动态概率统计器 107。

[0121] 总线 H408 连接熵解码器 106、动态概率统计器 107。总线 H 所传输的信息包括：1、字符概率预测值相关数据，从动态概率统计器 107 传至熵解码器 106；2、字符统计值更新信号，从熵解码器 106 传至动态概率统计器 107。

[0122] 总线 I409 连接连接动态概率统计器 107、熵解码器 106、系统对外界的数据端口。总线 I 所传输的信息包括：1、解密后的明文数据流，从熵解码器 106 传至动态概率统计器 107、数据端口；2、数据接收响应信号，从数据端口传至熵解码器 106。

[0123] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必要的硬件平台的方式来实现，当然也可以全部通过硬件来实施，但很多情况下前者是更佳的实施方式。软件包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例或者实施例的某些部分所述的方法。

[0124] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

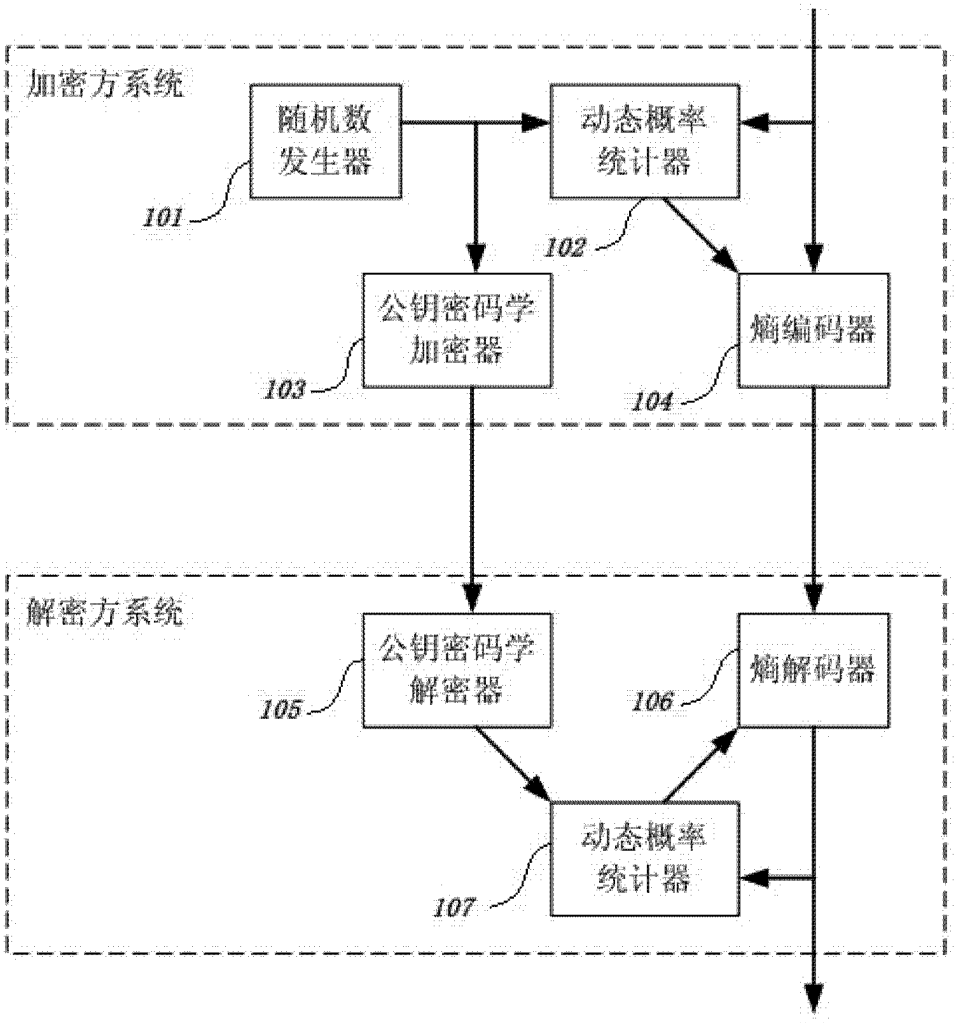

加密方系统
随机数发生器
101
动态概率统计器
102
公钥密码学加密器
103
熵编码器
104
解密方系统
公钥密码学解密器
105
熵解码器
106
动态概率统计器
107

图 1

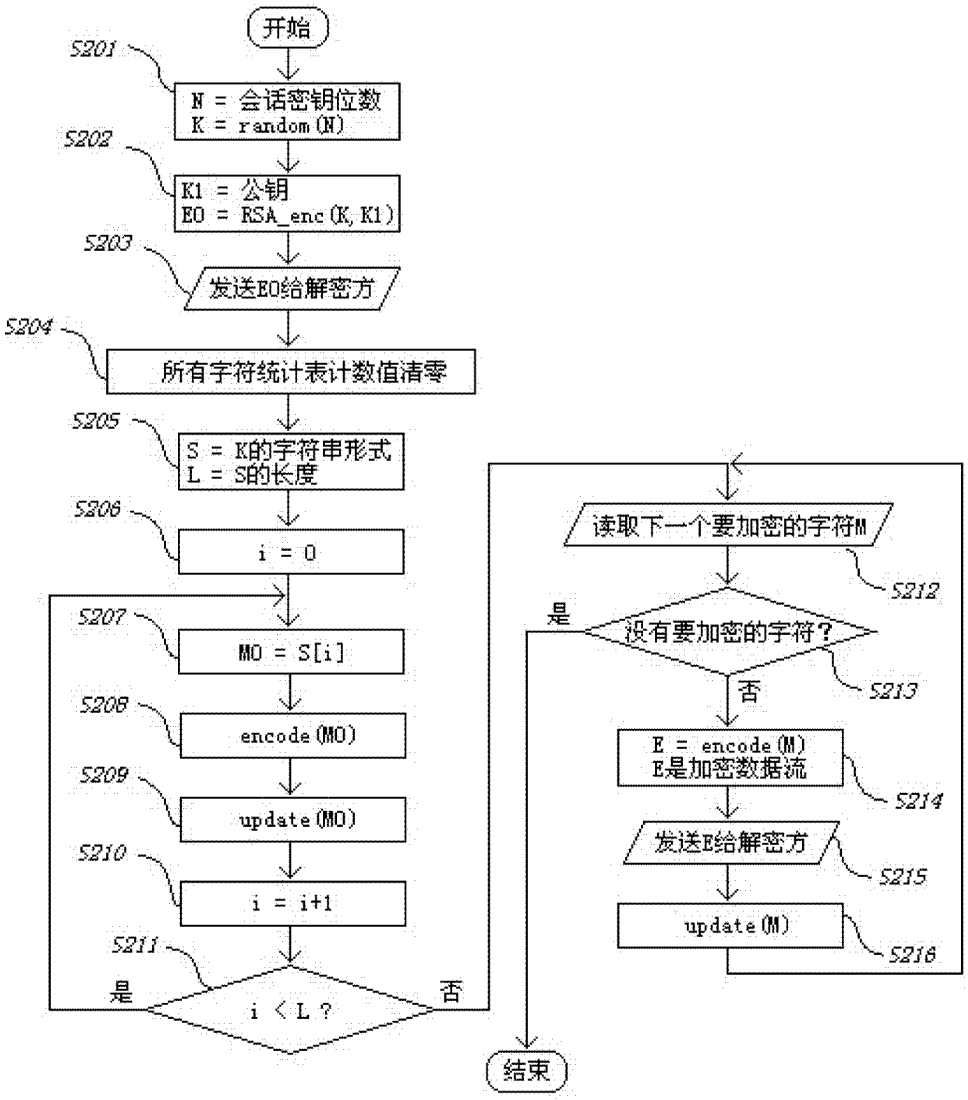

开始
S201
N = 会话密钥位数
K = random(N)
S202
K1 = 公钥
E0 = RSA_enc(K, K1)
S203
发送E0给解密方
S204
所有字符统计表计数值清零
S205
S = K的字符串形式
L = S的长度
S206
i = 0
S207
M0 = S[i]
S208
encode(M0)
S209
update(M0)
S210
i = i+1
S211
i < L ?
是
否
读取下一个要加密的字符M
S212
没有要加密的字符?
是
否
S213
E = encode(M)
E是加密数据流
S214
发送E给解密方
S215
update(M)
S216
结束

图 2

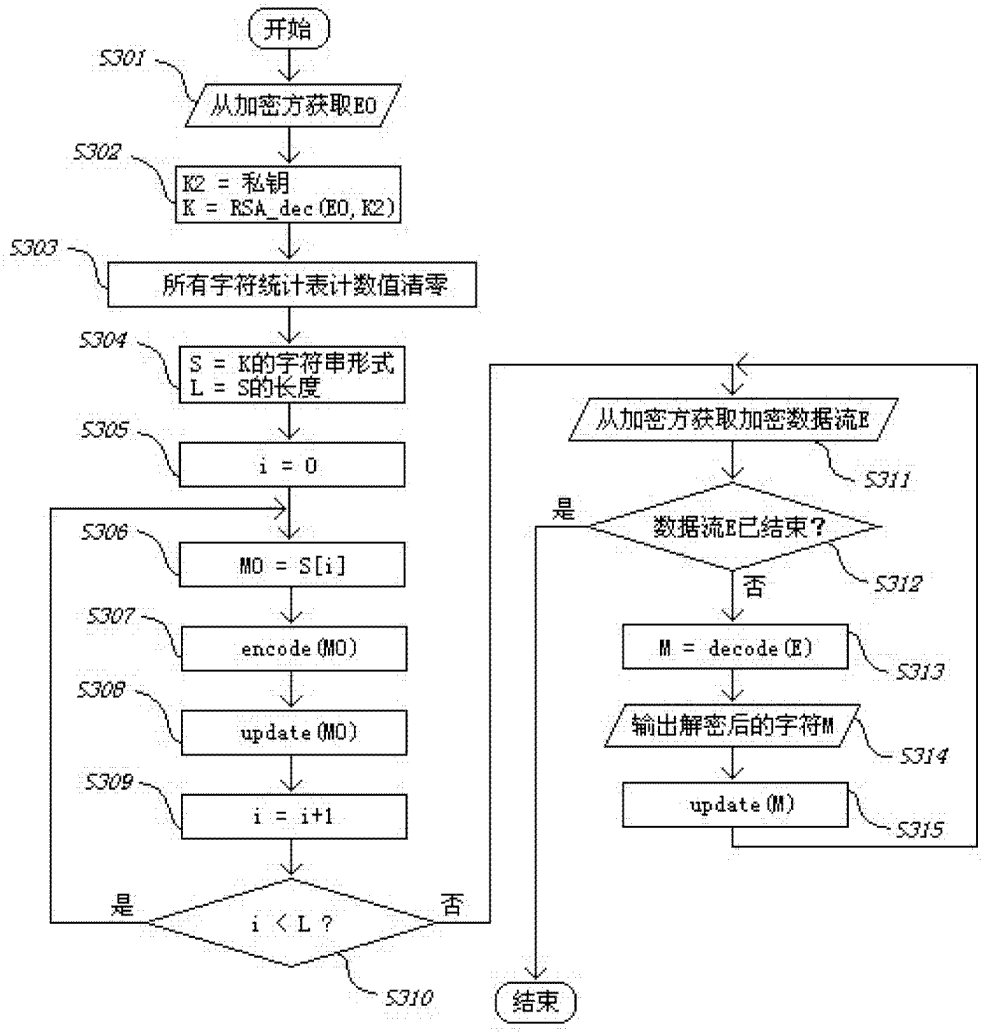

开始
S301
从加密方获取E0
S302
K2 = 私钥
K = RSA_dec(E0,K2)
S303
所有字符统计表计数值清零
S304
S = K的字符串形式
L = S的长度
S305
i = 0
S306
M0 = S[i]
S307
encode(M0)
S308
update(M0)
S309
i = i+1
是
i < L ?
否
S310
从加密方获取加密数据流E
S311
是
数据流E已结束?
S312
否
M = decode(E)
S313
输出解密后的字符M
S314
update(M)
S315
结束

图 3

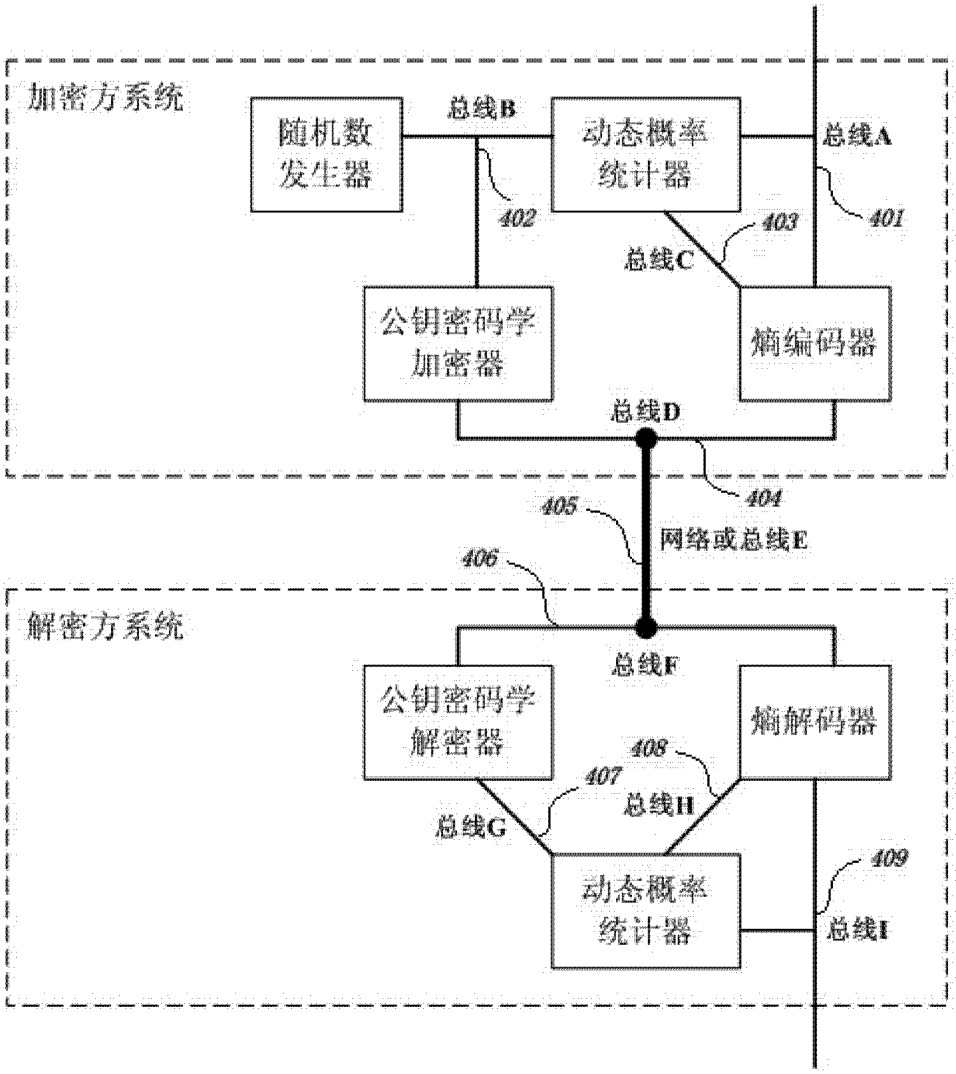

加密方系统
随机数发生器
总线B
动态概率统计器
总线A
402
401
403
总线C
公钥密码学加密器
熵编码器
总线D
404
405
网络或总线E
406
解密方系统
总线F
公钥密码学解密器
熵解码器
408
407
总线H
总线G
409
动态概率统计器
总线I

图 4