(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 10 月 31 日 (31.10.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/205407 A1

(51) 国际专利分类号:
H04L 9/06 (2006.01)

(21) 国际申请号: PCT/CN2018/104280

(22) 国际申请日: 2018 年 9 月 6 日 (06.09.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810363679.9 2018年4月22日 (22.04.2018) CN

(71) 申请人: 平安科技（深圳）有限公司 (**PING AN TECHNOLOGY (SHENZHEN) CO., LTD.**) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518033 (CN)。

(72) 发明人: 刘丹 (**LIU, Dan**); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518033 (CN)。

(74) 代理人: 北京市京大律师事务所 (**BEIJING JINGDA LAW FIRM**); 中国北京市西城区车公庄大街甲4号物华大厦A1706, Beijing 100080 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(54) **Title:** ENCRYPTION METHOD AND APPARATUS, AND COMPUTER DEVICE AND STORAGE MEDIUM

(54) **发明名称**: 加密方法、装置、计算机设备和存储介质

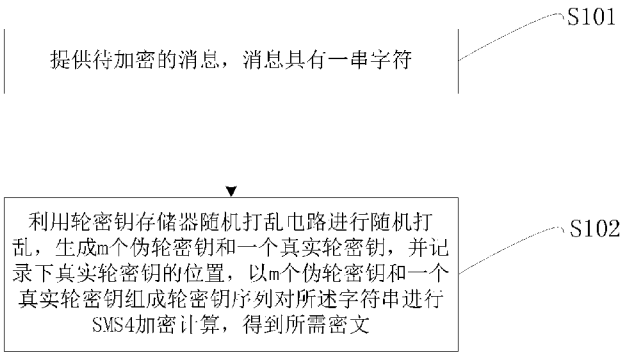


图 1

(57) **Abstract:** The present application relates to an encryption method and apparatus, and a computer device and a storage medium. The method comprises: acquiring a message to be encrypted, wherein the message has a string of characters; and carrying out random shuffling by using a random shuffling circuit of a round key memory, generating n pseudo round keys and one real round key, recording the position of the real round key, and carrying out SMS4 encryption calculation on the character string by means of a round key sequence formed by the n pseudo round keys and the real round key to obtain a required ciphertext. According to the method and apparatus, the amount of calculation of an algorithm is small, the encryption speed is high, the encryption efficiency is high, a long key is hard to crack when used, and the performance, security and reliability are also high, thus making up for the deficiency of security in the prior art.

WO 2019/205407 A1

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本申请涉及一种加密方法、装置、计算机设备和存储介质，所述方法包括：获取待加密的消息，所述消息具有一串字符；利用轮密钥存储器随机打乱电路进行随机打乱，生成n个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以n个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行SMS4加密计算，得到所需密文。上述方法及装置具有算法计算量小，加密速度快且加密效率高，使用长密钥时的难破解，同时具有高性能、高安全性、高可靠性，弥补了现有技术在安全性上的不足。

加密方法、装置、计算机设备和存储介质

本申请要求于2018年04月22日提交中国专利局、申请号为201810363679.9、发明名称为“加密方法、装置、计算机设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及信息安全等领域，尤其涉及一种加密方法、装置、计算机设备和存储介质。

背景技术

客户关系管理系统(CRM)提供了创建和维护客户清晰概况所需的工具和能力，包括从第一次接触到购买和售后。对于复杂的组织，CRM 系统可以提供帮助改善销售、市场营销、和/或客户服务组织发现新的客户目标、管理市场营销活动、以及驱动销售活动的特征和能力。

随着 CRM 解决方案的进步，实现了各种组合模式的通信，例如，即时消息收发、数据/应用共享、白板、以及可以与订户的在场以及可用性信息相结合的其它形式的通信。信息和数据的隐私安全成为最有价值的资产，各商业公司都会对自己系统内的数据读取做严格的信息保护，数据加密就是对信息进行保护的一种有效手段，能够阻止非授权用户的读取和传播。

然而，现有客户关系管理系统在客户消息交互过程中，存在的缺陷有非法绕开监管系统，直接读取未加密的客户消息，从而导致造成公司被投诉，客户流失。

发明内容

有鉴于此，有必要针对消息交互过程中，因未加密导致数据的安全保护性不高的问题，提供一种加密方法、装置、计算机设备和存储介质。

一种加密方法，包括：

获取待加密的消息，所述消息具有一串字符；

利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文。

一种加密装置，包括：

获取单元，设置为获取待加密的消息，所述消息具有一串字符；

加密单元，设置为利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文。

一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行上述加密方法的步骤：

获取待加密的消息，所述消息具有一串字符；

利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文。

一种存储有计算机可读指令的存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行上述加密方法的步骤：

获取待加密的消息，所述消息具有一串字符；

利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文。

上述加密方法、装置、计算机设备和存储介质，通过获取待加密的消息，所述消息具有一串字符，获取一个起始矩阵，根据寄存器号可以在相应的寄存器中获取矩阵起始地址和矩阵长度，再根据矩阵起始地址和矩阵长度在存储单元中获取相应地址存放的矩阵，该起始矩阵具有多列和多行，所述多行包括第一行和最后一行以及第一行与最后一行之间的中间行，以及最后一行中的所有

列中的不同字符和所有其他行中的所有列中的不同数字，并且其中所述字符串中的每个字符对应于矩阵的列之一。利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，所述轮密钥序列具体通过以下方式得到:确定真实轮密钥执行的序号，而轮密钥序列中其它 N 个伪轮密钥通过轮密钥随机选取，从轮密钥存储器的存储区中选择得到，所述 SMS4 加密计算是指将待加密的明文与轮密钥序列中的密钥依次进行轮函数迭代计算，得到所需密文，算法计算量小，加密速度快且加密效率高，使用长密钥时的难破解，同时具有高性能、高安全性、高可靠性，弥补了现有技术在安全性上的不足。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本申请的限制。

图 1 为本申请一个实施例中提供的加密方法的流程图；

图 2A 为本申请一个实施例中编码矩阵示意图；

图 2B 为本申请一个实施例中编码矩阵示意图；

图 3 为一个实施例中加密装置的结构框图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本申请的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、

元件、组件和/或它们的组。

作为一个较好的实施例，如图 1 所示，一种加密方法，该加密方法包括以下步骤：

步骤 S101,获取待加密的消息，消息具有一串字符;

获取要加密的消息，将消息数据转换为内容字符串。

步骤 S102,利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对字符串进行 SMS4 加密计算，得到所需密文。

通过密钥随机选取电路(或软件即软件调用模式实现)或通过密钥存储器随机打乱机构从密钥存储器中选择得到，n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文。首先需要保存 n 个伪轮密钥，这些伪轮密钥需要具有以下特点:伪轮密钥对应的每个字节是不同的，这个用来保证针对某个 S 盒的伪轮密钥是不一样的，S 盒为固定的 8 比特输入 8 比特输出的置换，记为 Sbox(.)，每次加密开始，把 n 个伪轮密钥和一个真实的轮密钥放在一起然后利用轮密钥存储器随机打乱电路进行随机打乱，记录下真实轮密钥的位置，即真实轮密钥执行的时刻，然后依次根据随机打乱的轮密钥开始执行 n 次轮函数，每次轮函数的结果都要进行保存，然后取真实的轮函数结果进入下一轮继续执行之后的运算。

在一个实施例中，获取待加密的消息，消息具有一串字符之后还包括：获取一个起始矩阵，根据寄存器号可以在相应的寄存器中获取矩阵起始地址和矩阵长度，再根据矩阵起始地址和矩阵长度在存储单元中获取相应地址存放的矩阵，该起始矩阵具有多列和多行，多行包括第一行和最后一行以及第一行与最后一行之间的中间行，其中最后一行中的所有列中的不同字符和所有其他行中的所有列中的不同数字，并且其中字符串中的每个字符对应于矩阵的列之一。

要获取一个矩阵时，根据寄存器号可以在相应的寄存器中获取矩阵起始地址和矩阵长度，再根据矩阵起始地址和矩阵长度在存储单元中获取相应地址存放的矩阵。矩阵运算指令包括一操作码和至少一操作域，其中，操作码用于指

示该矩阵运算指令的功能，矩阵运算单元通过识别该操作码可进行不同的矩阵运算，操作域用于指示该矩阵运算指令的数据信息，其中，数据信息可以是立即数或寄存器号。编码基于矩阵变换，在优选加密过程中，当使用矩阵内的字母时，从矩阵中的每个对应的值队列中除去与这些字母相关联的数字，直到队列为空。例如，如图 2A 和图 2B 所示，用的编码矩阵图，临时队列可以适合任何大小的队列。队列大小的最坏情况将是（（矩阵-1 中的行数）*（每行中值的数量））+1，使用这种方法，所有字符都可以被编码，包括 ASCII、国标字符集和信息编码。

在一个实施例中，轮密钥序列具体通过以下方式得到:确定真实轮密钥执行的序号，而轮密钥序列中其它 N 个伪轮密钥通过轮密钥随机选取，从轮密钥存储器的存储区中选择得到。

首先需要保存 n 个伪轮密钥，这些伪轮密钥具有下述特点,伪轮密钥对应的每个字节是不同的，这个用来保证针对某个 S 盒的伪轮密钥是不一样的，S 盒为固定的 8 比特输入 8 比特输出的置换，记为 Sbox(.)。每一次加密开始，把 n 个伪轮密钥和一个真实的轮密钥放在一起然后利用轮密钥存储器随机打乱电路进行随机打乱，记录下真实轮密钥的位置,即为真实轮密钥执行的时刻。然后依次根据随机打乱的轮密钥开始执行 n 次轮函数，每次轮函数的结果都要进行保存,然后得到真实的轮函数的结果。

在一个实施例中，SMS4 加密计算是指将待加密的明文与轮密钥序列中的密钥依次进行轮函数迭代计算，具体为:

设明文输入为（X0，X1，X2，X3）∈（Z232）4，密文输出为（Y0,Y1,Y2,Y3）∈（Z232）4,轮密钥为 rki∈Z232， i=0,1,2,…,31；则算法的加密变换为，

Xi+4=F（Xi,Xi+1,Xi+1,Xi+2,rki）=Xi T(Xi+1 Xi+2 Xi+3 rki),i=0,1,...,31;

(Y0，Y1，Y2，Y3)=R(X32，X33，X34，X35)=(X35，X34，X33，X32)。

SM4 分组密码算法，该算法为对称算法，密钥长度和分组长度均为 128 位，加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

设明文输入为（X0，X1，X2，X3）∈（Z232）4，密文输出为（Y0,Y1,Y2,Y3）∈（Z232）4,轮密钥为rki∈Z232， i=0,1,2,…,31；则算法的加密变换为，

Xi+4=F（Xi,Xi+1,Xi+1,Xi+2,rki）=Xi T(Xi+1 Xi+2 Xi+3 rki),i=0,1,...,31;

(Y0，Y1，Y2，Y3)=R(X32，X33，X34，X35)=(X35，X34，X33，X32)。

本算法的解密变换与加密变换结构相同，不同的仅是轮密钥的使用顺序。

加密时轮密钥的使用顺序为：（rk_0，rk_1，…，rk_{31}）

解密时轮密钥的使用顺序为：（rk_{31}，rk_{30},…，rk_0）

举例说明，对一组明文用密钥加密一次

明文：01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10

加密密钥：01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10

轮密钥与每轮输出状态：

rk[0] = f12186f9 X[0] = 27fad345

rk[1] = 41662b61 X[1] = a18b4cb2

rk[2] = 5a6ab19a X[2] = 11c1e22a

rk[3] = 7ba92077 X[3] = cc13e2ee

rk[4] = 367360f4 X[4] = f87c5bd5

rk[5] = 776a0c61 X[5] = 33220757

rk[6] = b6bb89b3 X[6] = 77f4c297

rk[7] = 24763151 X[7] = 7a96f2eb

rk[8] = a520307c X[8] = 27dac07f

rk[9] = b7584dbd X[9] = 42dd0f19

rk[10] = c30753ed X[10] = b8a5da02

rk[11] = 7ee55b57 X[11] = 907127fa

rk[12] = 6988608c X[12] = 8b952b83

rk[13] = 30d895b7 X[13] = d42b7c59

rk[14] = 44ba14af X[14] = 2ffc5831

rk[15] = 104495a1 X[15] = f69e6888

rk[16] = d120b428 X[16] = af2432c4

rk[17] = 73b55fa3 X[17] = ed1ec85e

rk[18] = cc874966 X[18] = 55a3ba22

rk[19] = 92244439 X[19] = 124b18aa

rk[20] = e89e641f X[20] = 6ae7725f

rk[21] = 98ca015a X[21] = f4cba1f9

rk[22] = c7159060 X[22] = 1dcdfa10

rk[23] = 99e1fd2e X[23] = 2ff60603

rk[24] = b79bd80c X[24] = eff24fdc

rk[25] = 1d2115b0 X[25] = 6fe46b75

rk[26] = 0e228aeb X[26] = 893450ad

rk[27] = f1780c81 X[27] = 7b938f4c

rk[28] = 428d3654 X[28] = 536e4246

rk[29] = 62293496 X[29] = 86b3e94f

rk[30] = 01cf72e5 X[30] = d206965e

rk[31] = 9124a012 X[31] = 681edf34

在一个实施例中，利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对字符串进行 SMS4 加密计算，得到所需密文之后还包括使用加密时用过的密钥及相同算法的逆算法对密文进行解密，使其恢复成可读明文。

需要说明的是，对称加密算法指的是加密和解密使用相同密钥的加密算法，算法是一组规则，规定如何进行加密和解密。在大多数的对称加密算法中，加密密钥和解密密钥是相同的。它要求发送方和接收方在安全通信之前，商定一个密钥。在对称加密算法中，数据发送方将明文（即原始数据）与加密密钥一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。接收方收到密文后，若想解读原文，则需要使用加密用过的密钥及相同算法的逆算法对密文进行解密，才能使其恢复成可读明文。

在一个实施例中，轮密钥存储器的存储区的初始状态为隐藏状态。

轮密钥存储器的存储区的初始状态为隐藏状态，解决了相关技术中对存储装置中数据的保护安全性不够高的问题，进而达到了提高存储装置中数据保护的安全性的效果。

如图 3 所示，在一个实施例中，提供一种加密装置，该加密装置包括：

获取单元，设置为获取待加密的消息，消息具有一串字符；

加密单元，设置为利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对字符串进行 SMS4 加密计算，得到所需密文。

在一个实施例中，获取单元还设置为获取一个起始矩阵，根据寄存器号可以在相应的寄存器中获取矩阵起始地址和矩阵长度，再根据矩阵起始地址和矩阵长度在存储单元中获取相应地址存放的矩阵，该起始矩阵具有多列和多行，多行包括第一行和最后一行以及第一行与最后一行之间的中间行，以及最后一行中的所有列中的不同字符和所有其他行中的所有列中的不同数字，并且其中字符串中的每个字符对应于矩阵的列之一。

在一个实施例中，加密单元还设置为确定真实轮密钥执行的序号 Q，而轮密钥序列中其它 N 个伪轮密钥通过轮密钥随机选取电路从轮密钥存储器的存储区中选择得到。

在一个实施例中，所述 SMS4 加密计算是指将待加密的明文与轮密钥序列中的密钥依次进行轮函数迭代计算，具体为：

设明文输入为（X_0，X_1，X_2，X_3）$\in$（Z_2^{32}）^{4}，密文输出为（Y_0, Y_1, Y_2, Y_3）$\in$（Z_2^{32}）^{4}，轮密钥为 $rk_i \in Z_2^{32}$，i=0, 1, 2, …, 31；则算法的加密变换为，

$X_{i+4}=F(X_i, X_{i+1}, X_{i+1}, X_{i+2}, rk_i)=X_i \quad T(X_{i+1} \quad X_{i+2} \quad X_{i+3} \quad rk_i)$, i=0, 1, . . . , 31；

$(Y_0, Y_1, Y_2, Y_3)=R(X_{32}, X_{33}, X_{34}, X_{35})=(X_{35}, X_{34}, X_{33}, X_{32})$。

在一个实施例中，所述加密单元还设置为使用加密时用过的密钥及相同算法的逆算法对密文进行解密，使其恢复成可读明文。

在一个实施例中，所述轮密钥存储器的存储区的初始状态为隐藏状态。

在一个实施例中，提出了一种计算机设备，所述计算机设备包括存储器和

处理器，存储器中存储有计算机可读指令，计算机可读指令被处理器执行时，使得处理器执行所述计算机程序时实现上述各实施例中加密方法中的步骤。

在一个实施例中，提出了一种存储有计算机可读指令的存储介质，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行上述各实施例中加密方法中的步骤。其中，存储介质可以为非易失性存储介质。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：只读存储器（ROM，Read Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁盘或光盘等。

以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本申请一些示例性实施例，其描述较为具体和详细，但并不能因此而理解为对本申请专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

权 利 要 求 书

1、一种加密方法，包括：

获取待加密的消息，所述消息具有一串字符；

利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文。

2、根据权利要求 1 所述的加密方法，其中，所述获取待加密的消息，所述消息具有一串字符之后还包括：

获取一个起始矩阵，根据寄存器号可以在相应的寄存器中获取矩阵起始地址和矩阵长度，再根据矩阵起始地址和矩阵长度在存储单元中获取相应地址存放的矩阵，该起始矩阵具有多列和多行，所述多行包括第一行和最后一行以及第一行与最后一行之间的中间行，其中最后一行中的所有列中的不同字符和所有其他行中的所有列中的不同数字，并且其中所述字符串中的每个字符对应于矩阵的列之一。

3、根据权利要求 1 所述的加密方法，其中，所述轮密钥序列具体通过以下方式得到:确定真实轮密钥执行的序号，而轮密钥序列中其它 N 个伪轮密钥通过轮密钥随机选取，从轮密钥存储器的存储区中选择得到。

4.根据权利要求 1 所述的方法，其中，所述 SMS4 加密计算是指将待加密的明文与轮密钥序列中的密钥依次进行轮函数迭代计算，具体为:

设明文输入为（X_0，X_1，X_2，X_3）∈（Z_2^{32}）^{4}，密文输出为（Y_0, Y_1, Y_2, Y_3）∈（Z_2^{32}）^{4}, 轮密钥为 $rk_i \in Z_2^{32}$，i=0, 1, 2, …, 31；则算法的加密变换为，

$X_{i+4}=F(X_i, X_{i+1}, X_{i+1}, X_{i+2}, rk_i)=X_i \quad T(X_{i+1} \quad X_{i+2} \quad X_{i+3} \quad rk_i)$, i=0, 1, . . . , 31；

$(Y_0, Y_1, Y_2, Y_3)=R(X_{32}, X_{33}, X_{34}, X_{35})=(X_{35}, X_{34}, X_{33}, X_{32})$。

5、根据权利要求 1 所述的加密方法，其中，所述利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文之后还包括使用加密时用过的密钥及相同算法的逆算法对密文进行解密，使其恢复成可读明文。

6、根据权利要求 3 所述的加密方法，其中，所述轮密钥存储器的存储区的

初始状态为隐藏状态。

7、一种加密装置，包括：

获取单元，设置为获取待加密的消息，所述消息具有一串字符；

加密单元，设置为利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文。

8、根据权利要求 7 所述的加密装置，其中，所述获取单元还设置为获取一个起始矩阵，根据寄存器号可以在相应的寄存器中获取矩阵起始地址和矩阵长度，再根据矩阵起始地址和矩阵长度在存储单元中获取相应地址存放的矩阵，该起始矩阵具有多列和多行，所述多行包括第一行和最后一行以及第一行与最后一行之间的中间行，以及最后一行中的所有列中的不同字符和所有其他行中的所有列中的不同数字，并且其中所述字符串中的每个字符对应于矩阵的列之一。

9、根据权利要求 7 所述的加密装置，其中，所述加密单元还设置为确定真实轮密钥执行的序号，而轮密钥序列中其它 N 个伪轮密钥通过轮密钥随机选取，从轮密钥存储器的存储区中选择得到。

10、根据权利要求 7 所述的加密装置，其中，所述 SMS4 加密计算是指将待加密的明文与轮密钥序列中的密钥依次进行轮函数迭代计算，具体为：

设明文输入为（X_0，X_1，X_2，X_3）$\in$（Z_2^{32}）^{4}，密文输出为（Y_0, Y_1, Y_2, Y_3）$\in$（Z_2^{32}）^{4}，轮密钥为 $rk_i \in Z_2^{32}$，i=0, 1, 2, …, 31；则算法的加密变换为，

$X_{i+4}=F(X_i, X_{i+1}, X_{i+1}, X_{i+2}, rk_i)=X_i \quad T(X_{i+1} \quad X_{i+2} \quad X_{i+3} \quad rk_i)$, i=0, 1, . . . , 31；

$(Y_0, Y_1, Y_2, Y_3)=R(X_{32}, X_{33}, X_{34}, X_{35})=(X_{35}, X_{34}, X_{33}, X_{32})$。

11、根据权利要求 7 所述的加密装置，其中，所述加密单元还设置为使用加密时用过的密钥及相同算法的逆算法对密文进行解密，使其恢复成可读明文。

12、根据权利要求 9 所述的加密装置，其中，所述轮密钥存储器的存储区的初始状态为隐藏状态。

13、一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机

可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行以下步骤：

获取待加密的消息，所述消息具有一串字符；

利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文。

14、根据权利要求 13 所述的计算机设备，其中，所述获取待加密的消息，所述消息具有一串字符之后，还使得所述处理器执行以下步骤：

获取一个起始矩阵，根据寄存器号可以在相应的寄存器中获取矩阵起始地址和矩阵长度，再根据矩阵起始地址和矩阵长度在存储单元中获取相应地址存放的矩阵，该起始矩阵具有多列和多行，所述多行包括第一行和最后一行以及第一行与最后一行之间的中间行，其中最后一行中的所有列中的不同字符和所有其他行中的所有列中的不同数字，并且其中所述字符串中的每个字符对应于矩阵的列之一。

15、根据权利要求 13 所述的计算机设备，其中，所述计算机可读指令被所述处理器执行时，使得所述处理器执行以下步骤：

确定真实轮密钥执行的序号，而轮密钥序列中其它 N 个伪轮密钥通过轮密钥随机选取，从轮密钥存储器的存储区中选择得到。

16、根据权利要求 13 所述的计算机设备，其中，所述 SMS4 加密计算是指将待加密的明文与轮密钥序列中的密钥依次进行轮函数迭代计算，具体为:

设明文输入为（X_0，X_1，X_2，X_3）∈（Z_2^{32}）^{4}，密文输出为（Y_0, Y_1, Y_2, Y_3）∈（Z_2^{32}）^{4}, 轮密钥为 $rk_i \in Z_2^{32}$，i=0, 1, 2, …, 31；则算法的加密变换为，

$X_{i+4}=F(X_i, X_{i+1}, X_{i+1}, X_{i+2}, rk_i)=X_i \quad T(X_{i+1} \quad X_{i+2} \quad X_{i+3} \quad rk_i)$, i=0, 1, . . . , 31；

$(Y_0, Y_1, Y_2, Y_3)=R(X_{32}, X_{33}, X_{34}, X_{35})=(X_{35}, X_{34}, X_{33}, X_{32})$。

17、一种存储有计算机可读指令的存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：

获取待加密的消息，所述消息具有一串字符；

利用轮密钥存储器随机打乱电路进行随机打乱，生成 n 个伪轮密钥和一个

真实轮密钥，并记录下真实轮密钥的位置，以 n 个伪轮密钥和一个真实轮密钥组成轮密钥序列对所述字符串进行 SMS4 加密计算，得到所需密文。

18、根据权利要求 17 所述的存储介质，其中，所述获取待加密的消息，所述消息具有一串字符之后，还使得一个或多个处理器执行以下步骤：

获取一个起始矩阵，根据寄存器号可以在相应的寄存器中获取矩阵起始地址和矩阵长度，再根据矩阵起始地址和矩阵长度在存储单元中获取相应地址存放的矩阵，该起始矩阵具有多列和多行，所述多行包括第一行和最后一行以及第一行与最后一行之间的中间行，其中最后一行中的所有列中的不同字符和所有其他行中的所有列中的不同数字，并且其中所述字符串中的每个字符对应于矩阵的列之一。

19、根据权利要求 17 所述的存储介质，其中，所述计算机可读指令被所述处理器执行时，使得一个或多个处理器执行以下步骤：

确定真实轮密钥执行的序号，而轮密钥序列中其它 N 个伪轮密钥通过轮密钥随机选取，从轮密钥存储器的存储区中选择得到。

20、根据权利要求 17 所述的存储介质，其中，所述 SMS4 加密计算是指将待加密的明文与轮密钥序列中的密钥依次进行轮函数迭代计算，具体为：

设明文输入为（X_0，X_1，X_2，X_3）∈（Z_2^{32}）^{4}，密文输出为（Y_0, Y_1, Y_2, Y_3）∈（Z_2^{32}）^{4}，轮密钥为 $rk_i \in Z_2^{32}$，i=0, 1, 2, …, 31；则算法的加密变换为，

$X_{i+4}=F(X_i, X_{i+1}, X_{i+1}, X_{i+2}, rk_i)=X_i \quad T(X_{i+1} \quad X_{i+2} \quad X_{i+3} \quad rk_i)$, i=0, 1, . . . , 31；

$(Y_0, Y_1, Y_2, Y_3)=R(X_{32}, X_{33}, X_{34}, X_{35})=(X_{35}, X_{34}, X_{33}, X_{32})$。

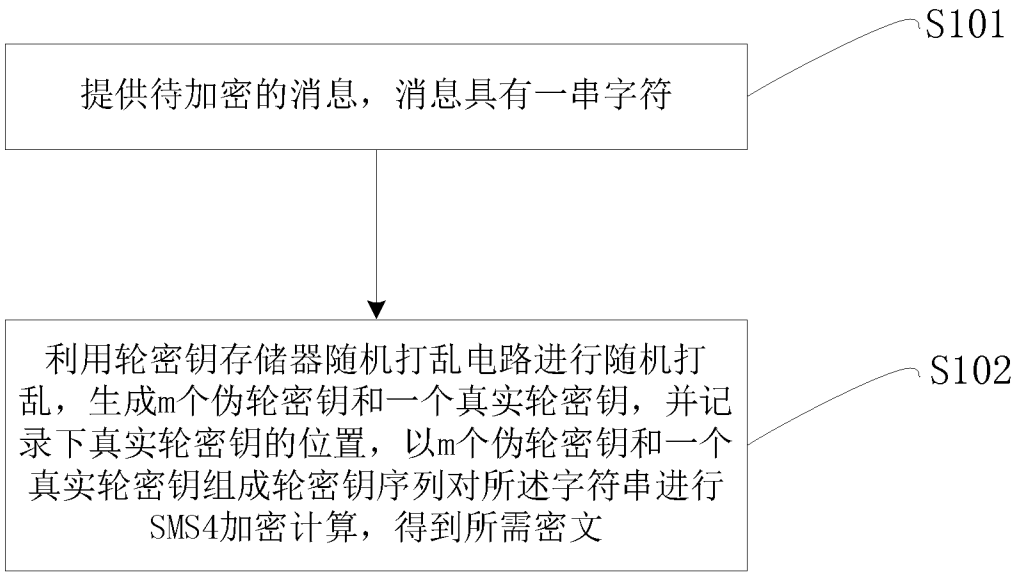


图 1

43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

图 2A

麓	蔽	毕	毙	毖	币	庇	痹	闭	敝	弊	必	辟	壁	臂	…
1745	1746	1747	1748	1749	1750	1751	1752	1753	1754	1755	1756	1757	1758	1759	
陛	匕	俾	荜	荸	薜	吡	哔	狴	庳	愎	滗	濞	弼	妣	…
1761	5616	5734	6074	6109	6221	6333	6357	6589	6656	6725	6868	6908	6986	6994	
斑	班	搬	扳	般	颁	板	版	扮	拌	伴	瓣	半	办	鲍	…
1663	1664	1665	1666	1667	1668	1669	1670	1671	1672	1673	1674	1675	1676	1711	

图 2B

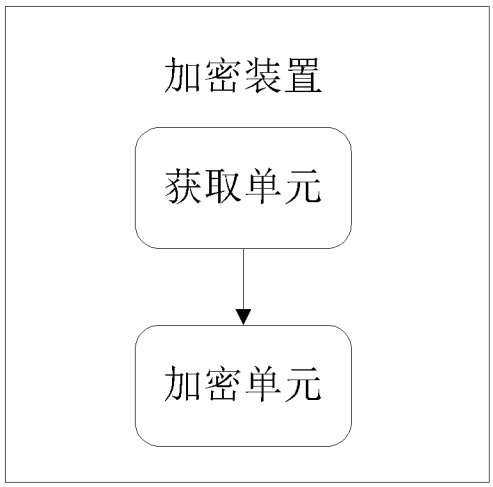


图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/104280

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNKI, CNPAT: 加密, sms4, 随机, 轮密钥, encrypt+, random, round key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104734842 A (SHANGHAI JIAO TONG UNIVERSITY ET AL.) 24 June 2015 (2015-06-24) description, paragraphs [0025]-[0043]	1-20
X	CN 104734845 A (SHANGHAI JIAO TONG UNIVERSITY ET AL.) 24 June 2015 (2015-06-24) description, paragraphs [0028]-[0052]	1-20
A	CN 101764684 A (GUANGZHOU GCI SCIENCE & TECHNOLOGY CO., LTD.) 30 June 2010 (2010-06-30) entire document	1-20
A	EP 2889760 A2 (INTEL CORPORATION) 01 July 2015 (2015-07-01) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 December 2018	**29 December 2018**

Name and mailing address of the ISA/CN	Authorized officer
National Intellectual Property Administration, PRC (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/104280

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 104734842 A	24 June 2015	None	
CN 104734845 A	24 June 2015	None	
CN 101764684 A	30 June 2010	None	
EP 2889760 A2	01 July 2015	US 2015186138 A1	02 July 2015

国际检索报告

国际申请号
PCT/CN2018/104280

A. 主题的分类

H04L 9/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L9

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI, EPODOC, CNKI, CNPAT:加密，sms4，随机，轮密钥，encrypt+，random，round key

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 104734842 A (上海交通大学 等) 2015年 6月 24日 (2015-06-24) 说明书第[0025]-[0043]段	1-20
X	CN 104734845 A (上海交通大学 等) 2015年 6月 24日 (2015-06-24) 说明书第[0028]-[0052]段	1-20
A	CN 101764684 A (广州杰赛科技股份有限公司) 2010年 6月 30日 (2010-06-30) 全文	1-20
A	EP 2889760 A2 (INTEL CORP.) 2015年 7月 1日 (2015-07-01) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 12月 19日	2018年 12月 29日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 陈红英 电话号码 86-(10)-53961636

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/104280

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
CN 104734842 A	2015年 6月 24日	无	
CN 104734845 A	2015年 6月 24日	无	
CN 101764684 A	2010年 6月 30日	无	
EP 2889760 A2	2015年 7月 1日	US 2015186138 A1	2015年 7月 2日