多密钥加密方法设计

衷宇清，王浩，林泽兵，王敏，陈立业
（广东电网有限责任公司广州供电局，广东 广州 510699）

摘　要：为了提高信息传输过程中的安全性，对当前的加密方法进行了研究，并介绍了通过对密钥进行处理增加加密安全性的研究现状。根据数据在发送和加密过程中要进行分段和分组的原理，设计了一种多密钥加密的方法：由源密钥和随机数生成分段密钥组和分组密钥组，由序号按匹配算法为每个分段和分组的数据选取相应密钥，实现多个密钥对信息传输过程中的加密。最后，一方面通过 MATLAB 测试验证该方法的加密效率，另一方面从理论和数学角度分析该方法的安全性并和传统方法进行对比，得到结论：该方法不需要太多开销即可在传统方法的基础上增加安全性。

关键词：信息安全；加密；密钥
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020304

Design of multi-key encryption method

ZHONG Yuqing, WANG Hao, LIN Zebing, WANG Min, CHEN Liye
Guangzhou Power Supply Bureau of Guangdong Power Grid Co., Ltd., Guangzhou 510699, China

Abstract: In order to improve the security in the process of information transmission, the current encryption methods were studied, and the research status was reported which increased the security of encryption by processing the key. According to the principle of segmenting and grouping data in the process of sending and encrypting, a method of multi-key encryption was designed: the segmenting key group and grouping key group were generated by the source key and random number, and the corresponding key was selected for each segmented and grouped data by its sequence number according to the matching algorithm. This method realized the encryption of multi-key in the process of information transmission. Finally, on the one hand, MATLAB was used to test and verify the encryption efficiency of this method. On the other hand, the security of this method was analyzed from the theoretical and mathematical perspective, comparing with the traditional method. It is concluded that this method can increase the security of the traditional method without too much cost much cost.

Key words: information security, encryption, key

收稿日期：2020−03−30；修回日期：2020−11−10
基金项目：中国南方电网有限责任公司科技项目（No.GZHKJXM20180038）
Foundation Item: Science and Technology Project of China Southern Power Grid Co., Ltd. (No.GZHKJXM20180038)

1 引言

信息加密是为了在不安全的传输环境中实现信息的安全传输，但是加密后攻击方同样有各种方法截获并破解传递的信息。不公开的加密算法容易出现各种漏洞，且不能保证安全，所以当前的加密算法大多都是公开的，当前的信息加密的安全性主要取决于密钥的安全。密码分析技术就是在不知道密钥和明文的情况下，通过对密文进行分析取得密钥，并最终恢复明文。当前数据加密主要依靠单密钥进行加密，如果攻击方采用各种方法对其进行破解之后，接下来所有的信息对攻击方来说都是透明的。

国内外在对称加密方面主要研究更加复杂和安全的加密算法，1977 年美国国家标准局确定了数据加密标准（data encryption standard，DES）算法，是现代密码学诞生的标志之一，揭开了商用密码研究的序幕。但随着技术发展，DES 已经不再安全，为了提高安全性能和充分使用 DES 已有的硬件软件资源，推出了多重 DES 加密算法（如 3DES）。但是 3DES 加/解密速度较慢，效率较低，因此高级加密标准（advanced encryption standard，AES）算法逐渐开始被使用，并到现在一直作为对称加密算法的标准。虽然加密算法的安全性越来越高，但是加密和破解是相互对立、共同发展的，以往被认为极其安全的加密算法也被逐一破解。当前的计算机运算能力越来越强大，可能当前的加密算法也都会被破解。并且随着物联网与卫星互联网技术的发展和广泛应用，通信不再仅仅是人与人之间的通信，物与物通信的比重逐渐加大，地面上的传感器和太空中的卫星由于其计算资源和存储资源比较匮乏，需要更加轻量化的加密算法，但是它们往往处于开放的环境中，其信息极易被截获，而轻量化的加密算法难以保障安全性，于是目前许多研究者将视线投向密钥，通过对密钥进行处理实现加密的复杂化。

目前在相关方面的研究主要有：参考文献[2]利用非同传数据包同步动态更新发送、接收双方的对称加密密钥，实现了加密过程中密钥的复杂化；参考文献[3]通过 7 bit 种子生成两个密钥，并利用这两个密钥对 64 bit 明文分组进行三重 TEA 加密；参考文献[4]通过从随机生成密钥集中选取任一密钥用于对返回地址进行加密，并设计了密钥迷惑位防止攻击方获取所有密钥后猜测密钥的指定位；参考文献[5]通过构建一个虚拟魔方，建立密钥与明文之间一一对应的关系，利用这种对应关系实现多密钥对明文的混合加密；参考文献[6]通过对密钥的多重哈希运算生成多个密钥，按顺序对明文数据块分配加密密钥，采取 ECB 工作模式来加密。

2 方案设计

2.1 方案原理

根据 OSI（open system interconnect，开放式系统互联）模型，网络通信的工作可以分为 7 层，其中传输层的作用是最关键的，它负责总体的数据传输和数据控制，提供端到端的交换数据的机制。传输层协议可以分为两种：面向连接的 TCP（transmission control protocol，传输控制协议）、面向非连接的 UDP（user datagram protocol，用户数据报协议）。TCP 要求在发送数据前建立端到端的连接，当数据交换完毕后释放已经建立的连接。根据 TCP，把要发送的数据划分为多个 TCP 报文段，并在首部附加序列号，实现不丢失、无重复的可靠交付服务。

因为分组加密只能对一定长度的数据进行加密，如果要对比较长的明文进行处理，就需要采用迭代的方法（又称工作模式）。而根据分组密码的工作模式，需要加/解密的数据划分为一定长度的明密文分组，由密钥或者其他参数对其进行连续或并行处理。

多密钥加/解密方法正是根据 TCP 划分报文

段，并有各自序列号可将其有序排列的原理，对各个数据报文段根据密钥匹配算法选取不同的分段密钥。并且在每个分段因分组加密需要将其划分为一定位数的明文分组，对这些固定长度有序排列的明文分组，同样可以根据密钥匹配算法选取不同的分组密钥。这样具体到某一分段的某一分组，就有两个密钥可以进行一定运算后对此分组进行加密。其他分段、其他分组同样依此方法进行操作，直到要发送的数据加密完毕后将其发送。

接收方通过发送方共享的参数自行生成发送方加密使用的密钥组，并根据同样的匹配算法选取相应分段分组的两个对应密钥，运算后根据约定的工作模式对密文进行解密，最终得到发送方加密前的明文。其中的过程如图 1 所示。

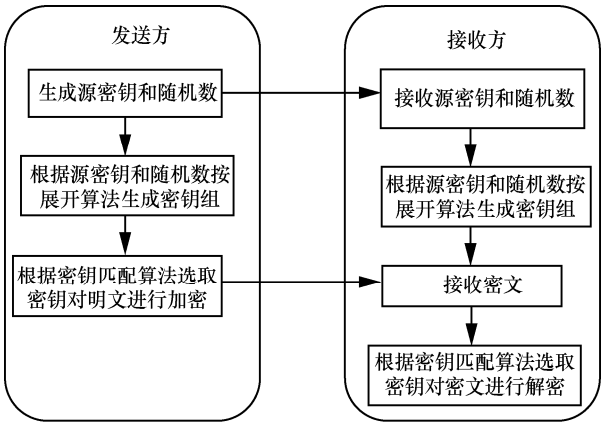

图 1　多密钥加解密方法过程

2.2　展开生成密钥组算法

多密钥加密方法的关键是采用了多个密钥对明文加密操作，以实现加密后密文的复杂度，让攻击方无法仅破解一个密钥就能解开所有密文。本算法的目的是根据共享的安全参数有效地展开生成多个不同且相互独立的密钥，并将其应用于接下来的对明密文匹配和加/解密操作中。

本算法要求具有易同步性、有序性、不可逆性、不相关性。

- 易同步性是指发送和接收双方可以很容易地根据相关参数通过本算法生成两份完全相同的密钥组。因为对称加密算法中的密钥是相同的，因此相同的密钥组是能够进行多密钥加/解密的必要条件。
- 有序性是指生成的密钥组密钥是可以进行有序排列的，这样进行加/解密钥匹配时可以有效地选择相应序号的密钥，实现了具体每个密钥的序号同步。
- 不可逆性是指攻击方无法通过产生的密钥去推算源密钥和随机数，如果这两个参数被攻击方破解，那么就完全获得了密钥组中所有的密钥。
- 不相关性是指每个密钥都与其前后产生的密钥是相互独立的，无法通过某种方法根据其中一个密钥去推算其他密钥的信息。只有这样才能实现多密钥加密的密钥复杂度。

本算法的步骤如图 2 所示，首先由源密钥 K_S 和随机数 $R+n$（n 的初始值为 1，生成一个密钥之后 n 自加 1）进行异或运算，接着把运算结果作为输入通过哈希函数运算：

$$\text{hash}[K_s \oplus (R+n)] \tag{1}$$

哈希函数运算是将输入的消息进行运算得到一定长度数值的算法，该算法保证无法通过输出值推算输入值：

$$\text{若 } y=\text{hash}(x)\text{，则 } x\underline{\text{难得出}}y \tag{2}$$

并且输入值即使变化 1 bit 也能对输出值产生巨大的扩散影响。因为传统的 MD5 哈希算法，已经不够安全，所以本文采取安全性和效率较为均衡的安全散列 SHA-1 算法，该算法输出的是固定的 160 bit 的哈希值。本方案采取的对称加密算法为密钥 128 bit 的 AES 算法，该算法目前安全性有所保证，并且比 AES-256 等算法有着更高的加密效率。因为哈希值位数与密钥所需位数不匹配，于是接下来将哈希值化分为左右两块（各 80 bit）：

$$(L\,/\,R)=\text{hash}[K_s \oplus (R+n)] \tag{3}$$

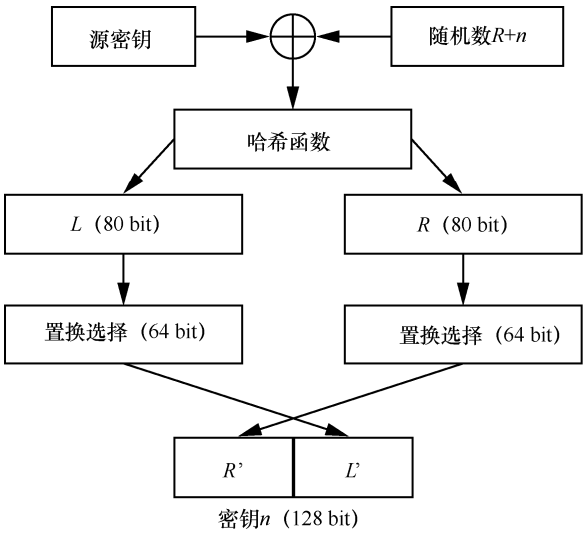

图 2　展开生成密钥组

并分别对其进行图 3 所示的置换选择（permutation selection，PS），该算法首先将 80 bit 数据按位数顺序映射到 8×10 的矩阵上，再将最左右两列数据与其同行相邻的数据异或运算形成 8×8 的矩阵，由从左至右、从上至下的顺序将处理后的矩阵化为 64 bit 的数据序列，依此法便生成了左右两块 64 bit 的数据序列：

$$L\underrightarrow{ps}L',R\underrightarrow{ps}R' \tag{4}$$

71 ⊕ 29	6	60	39	15	75	20	64 ⊕ 9
17 ⊕ 54	46	28	30	70	5	56	26 ⊕ 16
67 ⊕ 31	3	65	21	32	51	11	44 ⊕ 49
23 ⊕ 57	33	38	4	61	41	53	14 ⊕ 27
72 ⊕ 8	76	50	18	48	2	36	66 ⊕ 59
34 ⊕ 62	12	40	35	78	25	52	22 ⊕ 73
55 ⊕ 24	43	69	47	1	58	45	63 ⊕ 13
79 ⊕ 10	68	19	77	37	74	7	42 ⊕ 80

图 3　置换选择

再将其进行左右互换拼接，形成一个密钥：

$$K_n=(R'\mid L') \tag{5}$$

并重复上述过程共展开生成 256 个密钥，并且皆为 128 bit。

密钥分类如图 4 所示，再将 256 个密钥按序号奇偶拆开分别组成分段密钥和分组密钥各 128 个。

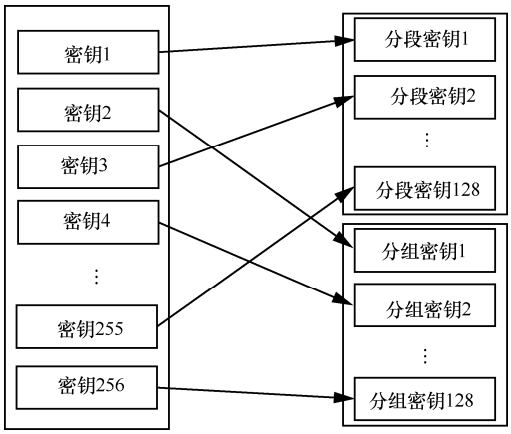

图 4　密钥分类

本算法仅通过共享源密钥和随机数，发送、接收双方按照算法所述步骤即可逐步生成满足要求的密钥组，简单有效，满足了易同步性。通过对随机数的累加操作，逐次地改变了哈希函数的输入值，有序地生成了多个密钥，并且能以累加的次数作为标注生成密钥的序号，实现了密钥的有序性。因为哈希函数具备不可逆、根据输入的变化产生广泛扩散的性质，并且通过了置换选择，因此密钥与密钥之间的关系变得非常复杂，实现了算法要求的不可逆性和不相关性。

2.3　加密工作模式

由于对称分组加密往往只能加密一定长度的数据（AES 为 128 bit，即 16 byte），而每个 TCP 报文在以太网分段可以长达约 1 500 byte，如果采用 128 bit 的密钥对此分段加密，则需要划分约 100 个明文分组，因此需要对分组加密算法进行迭代操作，又称加密工作模式。加密工作模式是进行多密钥加/解密方法的最直接的一步，正是在这种模式下具体体现了每个分段分组加密密钥的复杂性。

本设计的加密工作模式需要满足以下要求：隐藏性、高效率性、低传播性。

- 隐藏性是指即使有相同的明文，经过加密后的密文仍然是截然不同的，隐藏了明文的统计特性，可以防止统计分析攻击、代换攻击和分组重放攻击。
- 高效率性是指能够快速的处理大段的数据，缩短整体加解密的时间。
- 低传播性是指当密文分组某一分组出现错误后不会或者尽量少地影响后续分组的解密。

本方案的加密工作模式设计方案如图5所示，首先根据TCP报文段序号选取此分段对应的分段密钥 K_i，再根据分段中不同的分组选取对应的分组密钥 K_j，将两个密钥进行异或运算获取对此明文分组进行直接加密的密钥：

$$K = (K_i \oplus K_j) \tag{6}$$

最后将其对相应明文分组进行加密：

$$C_n = K(P_n) \tag{7}$$

因为是对明文进行分组后进行处理的，因此可以对多个明文分组同时进行加密操作。当密文到达接收方之后，接收方根据约定的密钥匹配方法选取同样的密钥运算后对相应的密文分组进行并行解密，最终获取明文：

$$P_n = K(C_n) \tag{8}$$

此加密工作模式采用的密钥是经过两个密钥运算过的结果，且不同分段的分段密钥不同，在同一分段的不同分组的其中一个密钥也是一直在变化的，因此进行加密的密钥取决于两个密钥组中的密钥和它们的密钥匹配算法。

由于对每个明文分组，加密的密钥是不同的。因此即使是相同的明文出现，它们的密文也会不同，满足了隐藏性。此加密工作模式还采用了并行的加密方式，不仅加快加/解密的操作速度，而且其中一个密文出现错误也与其他密文分组无关，满足了高效率性和低传播性要求。

2.4　密钥匹配算法

密钥匹配算法的作用在于为各分段分组根据其序号匹配相应的密钥，防止以往单密钥加密的方式。如果被攻击者获取密钥就可以完全解开密文的情况。要达成这点，同样要实现发送方和接收方的同步，因为本文所述的多密钥加解密方法需要用到上百个密钥，所以如何对相应分段分组的密钥进行选取是一个关键问

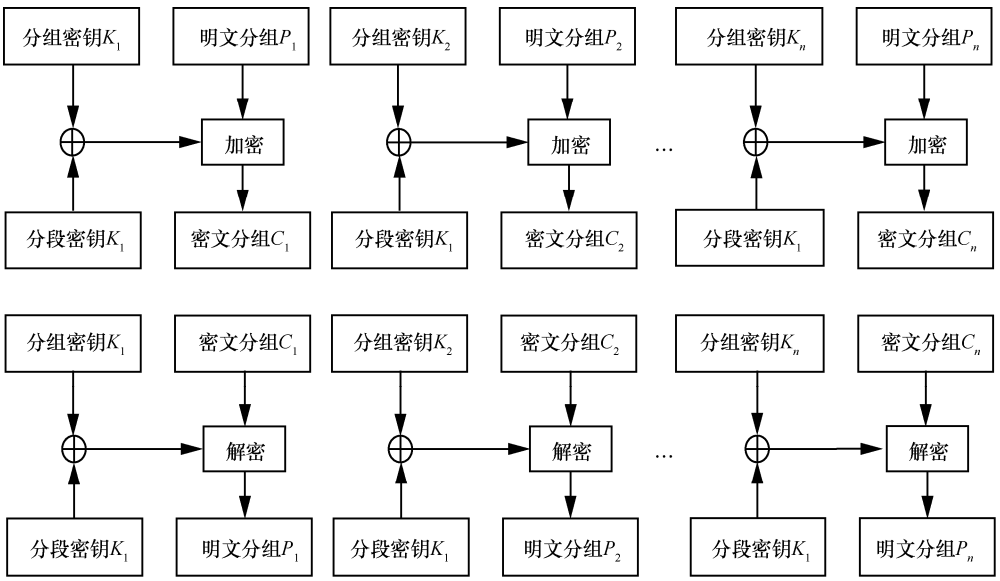

图 5　加密工作模式

题，如果仅采取简单的方法，攻击方可以很容易地分析得到规律并进行破解。因此密钥匹配算法的目的是根据共享参数的输入值的不同生成近乎随机的匹配方式，如果输入值能够进行有效的安全管理，那么在攻击方看来这种选择规律近乎是不可预测的。

本算法需要满足的性质有：易选取性和随机性。

- 易选取性是指算法能够很容易地通过输入分段分组序号变量得到要进行加/解密操作的确定的密钥序号输出，即容易选出对应的密钥。
- 随机性是指算法输出的密钥的具体选取无法预测，保证了密钥选取的复杂。

在 TCP 中，接收方收到的一个报文段序列号为上一个报文段序列号+该数据报文段所带数据的大小，因此收到的分段序号并不适合直接使用，需要对其进行标准化处理（即进行排序）后重新为每个分段分配 1、2、3…的标准序号。而在一个分段中，直接将每 128 bit 分组按顺序分配序号即可。密钥匹配如图 6 所示，将分段和分组的序号标准化处理后，可以将发送的消息近似看作一个矩阵，每个明文分组由其横坐标分段序号和纵坐标分组序号唯一确定，每个序号确定了一个与之对应的密钥，也就是说每个明文分组就分配了两个密钥负责对其进行加密。

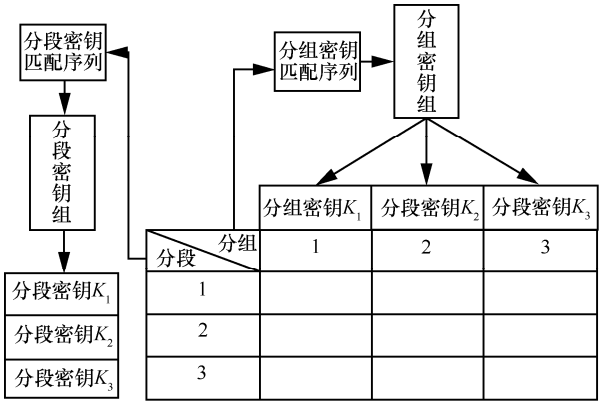

图 6　密钥匹配

进行密钥匹配首先需要生成两个密钥匹配序列，源密钥与随机数 $R-1$ 通过哈希函数运算生成分段密钥匹配序列，负责对不同分段进行匹配密钥选择：

$$S_i = \text{hash}[K_s \oplus (R-1)] \tag{9}$$

源密钥与随机数 $R-2$ 通过哈希函数运算生成分组密钥匹配序列，负责对不同分组进行匹配密钥选择：

$$S_j = \text{hash}[K_s \oplus (R-2)] \tag{10}$$

生成密钥匹配序列如图 7 所示。

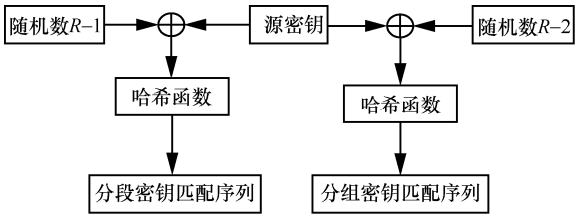

图 7　生成密钥匹配序列

而其中选取的方法如图 8 所示，分段密钥匹配序列和分段密钥匹配序列是两个各 160 bit 的 01 序列，从左端开始确定位数，每次根据分段和分组的序号递增向右逐次滑动 7 bit，每次选取的 7 bit 数字（2^7=128）化为 10 进制后+1 即要匹配的密钥的序号。若输入序号为 n，则输出的密钥序号的二进制为：$s_{7n}s_{7n+1}s_{7n+2}s_{7n+3}s_{7n+4}s_{7n+5}s_{7n+6}+1$，其中下标数值为在序列中的位数，$s$ 代表相应位置的数值，且当选取的位数要到达序列的末尾时，将 160 bit 的匹配序列复制拼接至正在使用的序列供其继续选取。

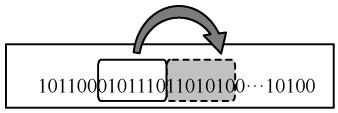

图 8　密钥匹配序列

本文所述密钥匹配算法，仅通过源密钥、随机数和两次哈希运算即可生成所需的匹配序列，选取密钥时只需要根据分段分组的序号顺序选定连续的 7 bit 向右做滑动得到 2 进制的密钥序号，

根据序号就可以找到匹配的密钥，满足了易选取性。本算法输出的密钥序号依赖于生成的哈希值，而哈希值的统计规律是无法预测的，其中的部分位就满足了随机性，并且 7 bit 的输出正好和分段分组密钥组容量相对应。

3　方案加密效率仿真验证测试

为了评估评估多密钥加/解密方法的加密效率，本文在 Win7、i5-7400CPU、8 GB 的环境上利用 MATLAB R2016a v9.0.0.34136 进行测试验证，每个数据都是取的 5 次执行的平均值。

展开生成密钥组的算法测试情况见表 1。

表 1　哈希函数采用 SHA-1 算法生成密钥组耗时情况

生成密钥个数/个	耗时/ms
64	98.09
128	200.569
256	389.512
512	780.690

根据表 1 中的数据分析，展开生成密钥组算法能够快速地通过源密钥和随机数有序地生成众多的密钥，并且本方法采取的生成 256 个密钥的方案，在不到 0.4 s 的时间内即可产生 16 384 种密钥组合，在密钥的复杂性和生成的效率中取得比较好的平衡。

在进行加密效率测试时，本文采取了与常规 AES 加密算法的 CBC（clipher block chaining，密码分组链接）工作模式进行对比，该模式具有良好的隐藏明文和易进行消息认证的特性，因此被广泛使用。加密效率测试情况对比见表 2。

表 2　加密效率测试情况对比

加密明文块数	本方法耗时/s	AES 加密算法 CBC 工作模式耗时/s	多耗时百分比
500	59.8	56	6.78%
1 000	120	113	6.19%
2 000	245	229	6.98%
3 000	370	347	6.62%

根据表 2 中的数据进行分析，因为 AES 加密算法自身为了隐藏明文和密钥的规律就足够复杂，因此多密钥加密方法在此基础上增加的密钥匹配算法和设计的加密工作模式的开销与其相比仅增加了 6%～7%，但却在此基础上增加了安全性。

4　方案安全性分析

在密码学领域有着著名的柯克霍夫原则：密码系统中的算法就算被攻击方所知，也无助于其用来推导出明文或密钥。也就是说，密码系统的安全不应该取决于不易改变的密码算法，而应该取决于可以随时改变的密钥。因此，在接下来对各种密码攻击类型的分析中，需要假设攻击方都已经掌握了相关算法，并逐渐增加攻击方掌握的有关资源，分析在依次增强的攻击类型中多密钥加密方法的安全性。虽然本方案设计的算法依托于 AES 算法，而 AES 可以抵抗线性分析和差分分析，但本方法的思想依旧可以用在其他对称加密算法中，因此在某些场景下也可利用 DES 进行安全分析。

4.1　攻击方只有密文

在这种情形下，攻击方最常采用的方法为穷举法，即不断尝试加密可能用到的所有密钥逐次对密文进行解密，直到能够从密文中获取明文，能解开此密文的输入值就是对称加密的密钥。

因为在常规的单密钥加密方案中，AES 算法密钥位数最少为 128 bit，穷举法需要进行尝试的次数为 2^{128} 次，目前是无法用穷举法来进行破解的。但正像在 DES 加密算法诞生后的若干年内，由于当时计算能力不够，被人认为其无法穷举，而现在已经能够轻松破解出其密钥，相信随着技术发展 AES 也会越来越受到挑战。

而在多密钥加密方案中，对每个明文分组匹配的密钥是不同的，攻击方利用穷举法破解其中一个密文分组得到密钥之后，无法利用此密钥解开其他密文分组，并且因为密钥生成算法的不可逆和无关联性无法据此推算其他密钥。在本方案

中攻击方需要尝试 2^{142}（$2^{128}\times2^{14}$）次，在单密钥加密方案的基础上增加了穷举的难度。

4.2 攻击方有若干数量的明密文对

在这种情形下，攻击方的任务就是通过明密文规律中推算出解密密钥或者导出一种能通过密文得到明文的替代算法。常用的方法为线性分析法，基本思想是以最佳的线性近似表达式来破译密码系统。

在常规的单密钥加密方案中，对明文分组的加密操作都与一个密钥有关，也就是说，攻击方可以轻易获取大量的由同一个密钥加密得到的明密文对，并利用其进行线性分析。以 DES 加密算法为例，目前可以在 2^{43} 个明密文对的条件下破译 DES。

但在多密钥加密方案中，进行线性分析的必要条件是获取由一个密钥加密得到的大量明密文对，而被同一个密钥加密的密文分组被稀释，攻击方难以获取足够多的有效明密文对来进行分析总结规律和推导替代算法。同样地，以 DES 为例，攻击方若想采取线性分析破解本方法，需要大量确定地用同一个密钥进行运算的明密文对，例如 1 号分段中的 1 号分组、1 号分段中的 161 号分组、161 号分段中的 1 号分组（分段分组密钥选取恰好经历了一个周期），而攻击方往往是难以获取到如此精确位置上的明密文对的，即使可以，在本方案中要想完全破解密文则至少需要 2^{57}（$2^{43}\times2^{14}$）个明密文对。

4.3 攻击方可以暂时控制加密机

在这种情形下，攻击方通过加密自己选定的明文消息获取对应的密文来确定密钥的结构或者密钥的相关信息。常用的方法为差分分析法，其基本思想是通过分析明文对差值对密文对差值的影响来恢复某些密钥比特。

在常规的单密钥加密方案中，攻击方可以构造自己想测试的明文来进行加密处理，密文都是由一个密钥运算生成因此，明文有一些轻微变化会在密文变化中得到一定的呈现。在 DES 中，破解需要 2^{47} 个选择明文和 2^{47} 次加密运算。

而在多密钥加密方案中，产生的密文的规律因为由不同的密钥产生所以被打乱，即使是相同的明文分组在不同的密钥加密后密文也是截然不同的，不同的明文分组被不同密钥加密后更是变得几乎毫无关联，得到的密文差分无法与明文差分建立联系。即使重复用一个分组进行测试破解得到密钥，这个密钥也只是众多密钥中的一个，难以进一步获取足够多的信息。同样以 DES 为例，破解本方案需要 2^{61}（$2^{47}\times2^{14}$）个选择明文和 2^{61} 次加密运算。

4.4 攻击方采取旁路攻击

理论上，目前的 AES 算法可以抵御除穷举外的其他密码分析，但易遭受旁路攻击造成密钥泄露。旁路攻击是一种绕开对复杂的加密算法的分析，利用密码算法的硬件实现运算中泄露的信息来破解密码系统。要达成这种攻击需要满足两个条件：（1）要将处理的数据与泄露的物理信号之间建立联系；（2）要将芯片中处理的数据与在信息泄露模型中处理的数据之间建立联系。根据条件可知，攻击方建立可靠的联系需要足够多的采样样本并且需要密钥相关状态的采样值。

在常规的单密钥加密方案中，加密时往往是一个密钥从始至终地进行众多次加密运算。密钥长时间的在硬件中对明文进行加密处理，就会不断地泄露相关的物理信号，攻击方通过持续地对其进行搜集采样和分析即可进行破解。

而在多密钥加密方案中，进行加密的密钥在每个分组是不同的，也就是说，每次加密时泄露的物理信号因密钥不同而不同，庞大的密钥个数不仅让攻击方难以获取足够多有效的样本，同时也让其难以建立可靠的联系。

4.5 攻击方获取密钥组中的密钥

当攻击方通过各种方法获取一个密钥组中的全部密钥时，由于其都是哈希函数的输出值，因此无法逆向推出源密钥和随机数。并且因为直接对明文分组加密的密钥是和另一个密钥组密钥异

或后的结果，所以攻击方获取的密钥组也无法直接用于对密文的解密。

若攻击方拥有两个密钥组的密钥，在这种情形下，虽然攻击方没有掌握具体的密钥匹配序列，但是可以采取将两组密钥一一相互异或运算的方法对密文进行尝试，虽然多密钥方法增加了一些被完全破解的复杂度，但此时密文从现实意义上已经被攻破了，因此要尽力避免两个密钥组中的密钥同时被攻击方获取。但从另一个角度来说，在本方案中获取全部密钥的难度要远远大于获取常规单密钥加密方法中获取唯一加密密钥的难度。

5　结束语

本文设计了一种多密钥的加密方法，利用 MATLAB 进行该方案的效率测试和测试对比，并根据柯克霍夫原则进行安全性分析。该方法根据共享的源密钥和随机数，通过一定算法展开生成通信双方同步的密钥组和密钥匹配序列，根据分段与分组的序号通过密钥匹配序列选取对应的密钥，两个密钥进行异或运算后作为直接加密的密钥对明文分组进行加密，得到由不同密钥进行加密的密文。经过效率验证和安全性分析，本文所述方法通过较小的开销即在传统的加密算法上增加了安全性。

参考文献：

[1] 王保仓, 贾文娟, 陈艳格. 密码学现状、应用及发展趋势[J]. 无线电通信技术, 2019, 45(1): 1-8.
WANG B C, JIA W J, CHEN Y G. Status quo, application and trend of cryptography[J]. Radio Communications Technology, 2019, 45(1): 1-8.

[2] 马李翠, 黎妹红, 吴倩倩, 等. 智能电网通信中动态密钥加密方法的研究与改进[J]. 北京邮电大学学报, 2017, 40(4): 74-79.
MA L C, LI M H, WU Q Q, et al. Research of dynamic key encryption algorithm in smart grid communication[J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(4): 74-79.

[3] 钟杨源, 江典棋, 刘伟城, 等. 一种可变密钥多重加密方法: CN106230580A[P]. 2016-12-14.
ZHONG Y Y, JIANG D Q LIU W C, et al. A multiple encryption method with variable key: CN106230580A[P]. 2016-12-14.

[4] 陈林博, 江建慧, 张丹青. 用多密钥加密方法防御面向返回编程的攻击[J]. 高技术通讯, 2014, 24(4): 355-364.
CHEN L B, JIANG J H, ZHANG D Q. Using multi key encryption to defend against the attack of return oriented programming[J]. Chinese High Technology Letters, 2014, 24(4): 355-364.

[5] 杨志国. 基于魔方的混合加密算法及应用研究[D]. 兰州: 兰州大学, 2010.
YANG Z G. Study on hybrid encryption algorithm based on the cube and application[D]. Lanzhou: Lanzhou University, 2010.

[6] 张光斌, 张永光, 王海滨, 等. 分组多密钥加密方法及装置: CN103716157A [P]. 2014-04-09.
ZHANG G B, ZHANG Y G, WANG H B, et al. Block multi key encryption method and device: CN103716157A[P]. 2014-04-09.

[7] 王健全, 马彰超, 李新中, 等.量子保密通信网络架构及移动化应用方案[J].电信科学, 2018, 34(9): 10-19.
WANG J Q, MA Z C, LI X Z, et al. Quantum secure communication network architecture and mobile application solution[J]. Telecommunications Science, 2018, 34(9): 10-19.

[8] 王栋, 李国春, 俞学豪, 等. 基于量子保密通信的国产密码服务云平台建设思路[J]. 电信科学, 2018, 34(7): 171-178.
WANG D, LI G C, YU X H, et al. Construction contemplation of cloud platform for domestic password service based on quantum secret communication[J]. Telecommunications Science, 2018, 34(7): 171-178.

[作者简介]

衷宇清（1968− ），男，广东电网有限责任公司广州供电局通信中心高级工程师，主要研究方向为电力通信。

王浩（1986− ），男，广东电网有限责任公司广州供电局通信中心高级工程师，主要研究方向为电力通信。

林泽兵（1988− ），男，广东电网有限责任公司广州供电局通信中心工程师，主要研究方向为电力通信。

王敏（1971− ），女，广东电网有限责任公司广州供电局通信中心高级工程师，主要研究方向为电力通信。

陈立业（1989− ），男，广东电网有限责任公司广州供电局通信中心工程师，主要研究方向为电力通信。