【电子与信息科学 / Electronics and Information Science】

基于 4 阶正交拉丁方组实际基本密码系统设计

田传俊

深圳大学电子与信息工程学院, 广东深圳 518060

摘 要: 研究 4 阶正交拉丁方组所确定的基本理论密码系统的实际模型设计方法. 基于计算机中简单易实现的几种运算, 提出 4 阶正交拉丁方组非统一代数式的构造方法, 并给出基本实际密钥空间 K 长度分别为 2、3 和 4 bit 时的实际基本密钥空间和统一形式的非线性加解密变换的设计方法. 所设计的 3 种非线性基本实际密码系统不同于现有常用的基于模加法运算所设计的线性基本密码系统, 可以将它们作为今后设计新流密码算法时所用的基本密码系统.

关键词: 信息安全技术; 密码学; 保密通信系统; 流密码算法; 4 阶正交拉丁方组; 基本实际密码系统
中图分类号: TN918 **文献标志码:** A **doi:** 10.3724/SP.J.1249.2020.03251

Design of practical basic cryptosystem based on four-order orthogonal Latin square group

TIAN Chuanjun

College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, Guangdong Province, P. R. China

Abstract: We propose the construction methods with non-uniform formulae for a group of four-order orthogonal Latin squares and give the methods of designing three basic practical key spaces with different bit lengths of 2, 3 and 4 bits and the corresponding encryption and decryption transformations by using several simple and easy operations in computers. The designed nonlinear basic practical cipher systems, which are different from the commonly used linear cryptosystems based on modular addition operation, can be used as the basic cryptosystem to design new stream cipher cryptosystems in the future.

Key words: technology of information security; cryptology; secure communication system; stream cipher algorithm; four-order orthogonal Latin square group; basic practical cipher system

当前, 密码学已成为数字信息安全领域的一门重要基础理论, 其中, SHANNON 创立的保密通信理论是现代密码学中最重要基础理论之一^[1-5]. 2018 年, 笔者对 SHANNON 保密通信理论的部分内容进行了重新解释^[6-7], 利用无限完善保密系统概念建立了比现有完善保密系统更一般的数学模型, 丰富了实用流密码系统的设计方法. 文献[6]将密

码算法设计分为基本密码系统 and 应用系统两个相对独立的设计步骤. 为使整个应用密码(或保密通信)系统具有完善保密性, 可利用正交拉丁方组设计相关基本密码系统中的理论密钥空间, 但这会使相关的实际密钥空间及其加解密变换的设计更加复杂. 因此, 研究基于拉丁方组的密钥空间的设计方法十分必要. 考虑到文献[6]并未对实际基本密钥空间

Received: 2019-04-24; Accepted: 2019-07-23

Foundation: National Natural Science Foundation of China (61070252)

Corresponding author: Professor TIAN Chuanjun. E-mail: tiancj@szu.edu.cn

Citation: TIAN Chuanjun. Design of practical basic cryptosystem based on four-order orthogonal Latin square group [J]. Journal of Shenzhen University Science and Engineering, 2020, 37(3): 251-256. (in Chinese)

与加解密变换设计进行深入细致的研究, 本研究提出基本实际密码模型的具体设计方法, 以便为设计应用保密通信系统打下部分基础.

常用的基本密码系统都是利用 1 bit 明密文空间上的线性函数设计的^[6-9]. 因此, 利用 2 bit 或多 bit 明密文空间上的非线性函数来设计基本密码系统就是全新的方法, 可作为序列密码算法的重要组成部分. 若将加密看成置乱编码, 则 1 bit 加密是标量置乱编码, 而多 bit 加密是矢量置乱编码, 矢量编码比标量编码要复杂得多. 当前对 2 bit 明密文空间上相关的多比特密钥空间设计的研究还未充分展开. 因此, 本研究拟讨论一类长度为 2 bit 或 4 元 (明密文空间) 非线性基本实际密码模型的设计问题, 该方法易于推广到更多 bit 基本密码系统中.

由文献[6]可知, 在 1 bit (明密文) 空间中, 现有流密码系统常用的基本密码系统, 是利用一个 2 阶拉丁方来设计其中关键的理论密钥空间的, 而在 2 bit 明密文空间中, 利用 4 阶拉丁方组可设计出更多的新基本密码系统. 考虑到利用 4 阶及其以上阶拉丁方组比利用 2 阶拉丁方来设计基本密码系统或其理论密钥空间要复杂得多, 本研究重点研究基于 4 阶正交拉丁方组的基本实际模型设计的问题.

1 记号和概念

参照文献[6-7], 将基本密码系统的理论模型表示为 (M, C, T) 或 (M, C, T, T^{-1}) , 并将与之对应的实际模型表示为 (M, C, K, E, D) . 其中, M 和 C 为 (基本) 明文和密文空间; T 为基本理论加密密钥空间; K 为实际密钥空间; E 为 (基本) 加密变换; D 为解密变换. 在实际应用中, 对于某个基本密码系统, 设计的基本理论 (密码) 模型 (M, C, T) 和相应的基本实际 (密码) 模型 (M, C, K, E, D) 应满足如下关系: T 可利用 (K, E) 来实现或表示, 但 T 可利用多种不同形式的 K 和 E 来实现, 逆变换 T^{-1} 类似.

用小写字母表示基本明文和密文与实际密钥空间的元素或单元, 如 $m \in M$, 则对明文 m 加密可表示为 $c = T(m) = E(k, m) = E_k(m) \in C$, 解密也类似表示.

参照文献[2-6]和计算机实际应用现状, 通常将 M 和 C 设计为由某个长度的 (所有) 不同 bit (向量或序列) 组成的同一个集合, 因而其设计会很简单. 设计基本密码系统就是设计理论或实际密钥空

间和加解密函数. 为便于应用, K 通常会被设计为一个较短消息组成的集合, 而 E 和 D 会被设计为一组易于计算机实现的规则或运算, 且最好做到 E 和 D 相同. K 最好能设计为由某个长度的所有不同比特向量组成的集合, 正如数据加密标准 (data encryption standard, DES) 算法中的实际密钥空间是由 (几乎) 所有不同的 56 bit 向量组成的集合一样.

设计基本密码系统的实际模型 (M, C, K, E, D) 要基于理论模型 (M, C, T) , 并利用正交拉丁方组设计该理论模型^[6]. 为设计出与理论模型对应的实际模型, 先解释一下理论模型中每个理论密钥可逆变换的表示方法和正交拉丁方组的基本知识.

在实际的计算机保密通信技术应用中, 常将相同的有限基本明文和密文空间设计为 $M = C = Z_2^n = \{0 \cdots 00, 0 \cdots 01, \cdots, 1 \cdots 11\} = Z_{2^n} = \{0, 1, \cdots, 2^n - 1\}$. 其中, $n = 1, 2, \cdots$. 为了方便, 将 Z_2^n 和 Z_{2^n} 中的相应元素看成两种不同表示形式的同一个数值, 则每个可逆 (理论密钥) 变换或函数可用多种形式表示, 通常用函数计算式 (或代数式)、表格式或矩阵式表示. 例如, 在 $M = C = Z_{2^2} = \{0, 1, 2, 3\}$ 上, 模 4 加 1 运算所决定的可逆变换 $\tilde{T}: M \leftrightarrow C$, 可利用函数计算式、表格式和矩阵式分别表示为: $c = \tilde{T}(m) = E_1(m) = (m + 1) \bmod 4, m \in M, \bmod 4$ 为模 4 运算、

0	1	2	3
1	2	3	0

 或 $\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{bmatrix}$. 其中, 在表格式和矩阵式中, 第 1 行为基本明文空间中每个明文单元数值 (对其递增排序称为自然排序), 第 2 行对应位置的元素是将每个明文单元变换后得到的数字. 若规定明文单元总表示为自然排序, 则在矩阵式或表格式中, 可将第 1 行的所有明文省略不写, 进而利用一个矩阵表示多个可逆 (加密或解密) 变换. 例如, 利用式 (1) 的每个 4 阶矩阵都能表示 Z_{2^2} 上 4 个不同的非线性可逆变换.

$$L_1 = \begin{bmatrix} 0 & 3 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{bmatrix}, L_2 = \begin{bmatrix} 3 & 1 & 0 & 2 \\ 2 & 0 & 1 & 3 \\ 0 & 2 & 3 & 1 \\ 1 & 3 & 2 & 0 \end{bmatrix},$$

$$L_3 = \begin{bmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 2 \\ 3 & 2 & 0 & 1 \\ 2 & 3 & 1 & 0 \end{bmatrix} \quad (1)$$

需要强调的是, 每个 Z_{2^2} 或 $Z_n = \{0, 1, \cdots, n - 1\}$ 上可逆变换的函数计算式都不是唯一的, 但其表格式和矩阵式都是唯一的 (在不管排序的情况

下), 其中, $n = 2, 3, \dots$. 同一个可逆变换的函数计算式形式不同, 其计算量也不同. 因此, 在实际应用中计算量最少或容易实现的计算式更会受到关注. 表格式和矩阵式的唯一性有利于描述和研究变换或函数的一些本质特性, 在理论研究中具有重要作用. 尽管表面上函数计算式的多样性和灵活性会给理论研究带来不少困惑和麻烦, 但因具有适于计算机应用等特点常被用于实际应用中. 同时, 函数计算式的实用性也易导致在实用的密码算法设计中只注重设计算法的实际模型, 难见用“先理论模型、后实际模型”(或“理论与实际模型”并重)方法设计常用密码算法. 因此, 本研究基于文献[6]利用“理论与实际模型”并重的方法设计几种新的基本密码系统.

设 $A = (a_{ij})_{n \times n}$ 和 $B = (b_{ij})_{n \times n}$ 都是由数集 $Z_n = \{0, 1, \dots, n-1\}$ 中的数字构成的 n 阶矩阵, 将 A 和 B 构成的矩阵对 (A, B) 记为

$$(A, B) = \begin{bmatrix} (a_{11}, b_{11}) & (a_{12}, b_{12}) & \cdots & (a_{1n}, b_{1n}) \\ (a_{21}, b_{21}) & (a_{22}, b_{22}) & \cdots & (a_{2n}, b_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ (a_{n1}, b_{n1}) & (a_{n2}, b_{n2}) & \cdots & (a_{nn}, b_{nn}) \end{bmatrix} \quad (2)$$

下面给出拉丁方及其正交组的相关概念.

定义1 设 $n \in \{2, 3, 4, 5, \dots\}$, 若 Z_n 上所有不同的数字在 n 阶方阵 L 的每行和每列中都出现, 则称 L 为 n 阶拉丁方.

定义2 若 A 和 B 都是由数字 $0, 1, 2, \dots, n-1$ 构成的 n 阶方阵, 且矩阵对 (A, B) 的所有元素正好为 $Z_n^2 = \{(i, j) | i, j \in Z_n\}$, 则称 A 与 B 正交. 若 k 个拉丁方 $A_1, A_2, \dots, A_k$ 两两正交, $k = 2, 3, \dots$, 则称 $A_1, A_2, \dots, A_k$ 为正交拉丁方组.

由定义1和定义2, 可验证式(1)中的3个矩阵都是两两正交的4阶拉丁方, 且2阶拉丁方仅两个, 但它们并不正交. 为便于叙述, 本研究将由一个拉丁方组成的矩阵集合称为正交拉丁方组.

利用正交拉丁方组设计基本密码系统能在理论上保证整个保密通信系统在一定条件下具有完善保密性^[6]. 不过, 每个正交拉丁方组都只能用于直接设计密码系统的理论密钥变换空间, 相应的实际密钥空间及其加解密变换的设计方法却是复杂多样的. 下面将对这一问题展开研究.

2 基本实际密码模型的设计方法

以式(1)中的正交拉丁方组所决定的理论密钥

空间为例, 设计相应的实际密钥空间. 本研究设计方法可推广到其他类型的正交拉丁方组.

将基于式(1)中的一个或多个矩阵(对应的可逆变换组)所要设计的基本密码系统设为 (M, C, T) 和 (M, C, K, E, D) , 则基本明文空间 M 和基本密文空间 C 可用两种形式表示: ① 利用2 bit 数字表示为 $M = C = Z_2^2 = \{00, 01, 10, 11\}$; ② 利用十进制数字表示为 $M = C = Z_{2^2} = \{0, 1, 2, 3\}$. 将利用十进制数表示的明文单元记为 m , 将利用2 bit 表示的明文单元记为组合形式 $m_1 m_2$. 为了方便, 将这两种形式所表示的同一个数不加区别, 则有 $m = m_1 m_2$, 其中, $m_1, m_2 \in Z_2$; $m \in Z_{2^2}$. 密钥和密文遵循相同记法.

将式(1)中的3个拉丁方所决定的所有可逆变换按照从上到下、从左到右的顺序依次记为 $\{T_1, T_2, T_3, T_4\}, \{T_5, T_6, T_7, T_8\}$ 和 $\{T_9, T_{10}, T_{11}, T_{12}\}$. 甚至将明文省略, 则 $T_1, T_2, \dots, T_{12}$ 可用向量表示为 $T_1 = (0, 3, 1, 2), T_2 = (1, 2, 0, 3), \dots, T_{12} = (2, 3, 1, 0)$.

利用函数计算式表示上述可逆变换. 对任意 $m_1, m_2 \in Z_2$ 和 $m = m_1 m_2 \in Z_{2^2}$, 可逆变换 T_1 为 $c = T_1(m) = (m_1 \times m - m_2 - m_1 \times \bar{m}_2) \bmod 4$ (3) 其中, $\times$ 表示实数乘法; $-m_2 \bmod 4 = 4 - m_2 \in Z_{2^2}$; $-x$ 为 $x \in Z_{2^2}$ 的负元, 或表示实数减法中减去 x ; $\bar{m}_2$ 为对 $m_2 \in Z_2$ 进行取补运算.

采用类似方法, 可得其他可逆变换的代数式为

$$\begin{aligned} c &= T_2(m) = (m_2 \times m - m_1 + 1) \bmod 4 \\ c &= T_3(m) = (m_2 \times m - m_1 + 3) \bmod 4 \\ c &= T_4(m) = (m_1 \times m - m_2 - m_1 \times \bar{m}_2 + 2) \bmod 4 \\ c &= T_5(m) = (m_2 m_1 + 3) \bmod 4 \\ c &= T_6(m) = (m + m_1 + m_2 + 2) \bmod 4 \\ c &= T_7(m) = (m + m_1 + m_2) \bmod 4 \\ c &= T_8(m) = (m_2 m_1 + 1) \bmod 4 \\ c &= T_9(m) = (m_1 \times m - m_2 - m_1 \times \bar{m}_2 + 1) \bmod 4 \\ c &= T_{10}(m) = [(2 \times m_2 - 1) \times m_1 + m_2] \bmod 4 \\ c &= T_{11}(m) = (m_1 \times m - m_2 - m_1 \times \bar{m}_2 + 3) \bmod 4 \\ c &= T_{12}(m) = (m_2 \times m - m_1 + 2) \bmod 4 \end{aligned}$$

需要注意的是, 对任意 $x, y \in Z_2$, xy 和 $x \times y$ 意义并不相同. 可见, 式(1)中的每个拉丁方都可利用“非统一形式”的非线性代数计算式表示.

另外, $T_1^{-1} = T_7, T_2^{-1} = T_6, T_3^{-1} = T_8, T_4^{-1} = T_5$, 且 $T_9^{-1} = T_9, T_{10}^{-1} = T_{10}, T_{11}^{-1} = T_{12}, T_{12}^{-1} = T_{11}$. 因此, $\{T_1, T_2, T_3, T_4\}, \{T_5, T_6, T_7, T_8\}$ 和 $\{T_9, T_{10}, T_{11}, T_{12}\}$ 的所有逆变换的代数式也就容易确定了.

按照上述方式, Z_2^2 中的每个可逆变换都能利用代数式表示, 在此不再赘述. 不过, 3 bit 或 4 bit 等所确定的集合 Z_8 或 Z_{16} 等的所有可逆变换或拉丁方数量会非常多, 难以全部列举, 导致相关代数式也难以全部列出. Z_2^2 中每个可逆变换或拉丁方实际中都能明确写出其代数式的特点会在理论密钥变换空间设计时发挥特殊作用.

然后, 考虑基本实际密钥空间 K 和加解密函数 E 与 D 的设计. 与 1 bit 基本密码系统的密钥空间具有唯一性不同, 2 bit 基本密码系统的密钥空间呈多样性, 且密钥数量随正交拉丁方组数量的变化而变化. 若与应用密钥流序列空间特性结合, 还能提出新的研究方向. 下面将详述把 K 设计为长度为 2、3 和 4 bit 时的设计方法.

2.1 基本实际密码系统 1 ($M_1 = C_1 = K_1 = Z_2^2$, E_1 , D_1): 实际密钥空间 K_1 由 2 bit 组成

当 $K_1 = Z_2^2 = \{00, 01, 10, 11\}$ 时, 选择 L_3 所决定的 4 个可逆变换组 $\{T_9, T_{10}, T_{11}, T_{12}\}$ 作为基本理论密钥变换空间, 设计与基本实际密钥空间 $K_1 = Z_2^2$ 相应的加解密变换. 参照 T_9, T_{10}, T_{11} 和 T_{12} 的代数式, 可将基本实际密码系统 ($M_1 = C_1 = K_1 = Z_2^2$, E_1, D_1) 设计为:

1) 基本加密变换 E_1 : 对任一明文 $m = m_1 m_2 \in Z_2^2$ 和密钥 $k = k_1 k_2 \in Z_2^2$, 其中, $m_1, m_2, k_1, k_2 \in Z_2$, 设 $\wedge$ 为逻辑与运算, 且 $\bar{x} = 1 - x$ 为逻辑补 (或者逻辑非) 运算, 对任意 $x \in Z_2$, 将 E_1 设计为

$$c = E_1(k, m) = [(\bar{k}_1 \wedge \bar{k}_2) \times T_9(m) + (\bar{k}_1 \wedge k_2) \times T_{10}(m) + (k_1 \wedge \bar{k}_2) \times T_{11}(m) + (k_1 \wedge k_2) \times T_{12}(m)] \bmod 4 \quad (4)$$

2) 基本解密变换 D_1 : 对任一密文 $c = c_1 c_2 \in Z_2^2$ 和密钥 $k = k_1 k_2 \in Z_2^2$, 其中, $c_1, c_2, k_1, k_2 \in Z_2$, 将 D_1 设计为

$$m = D_1(k, c) = [(\bar{k}_1 \wedge \bar{k}_2) \times T_9^{-1}(c) + (\bar{k}_1 \wedge k_2) \times T_{10}^{-1}(c) + (k_1 \wedge \bar{k}_2) \times T_{11}^{-1}(c) + (k_1 \wedge k_2) \times T_{12}^{-1}(c)] \bmod 4 = [(\bar{k}_1 \wedge \bar{k}_2) \times T_9(c) + (\bar{k}_1 \wedge k_2) \times T_{10}(c) + (k_1 \wedge \bar{k}_2) \times T_{11}(c) + (k_1 \wedge k_2) \times T_{12}(c)] \bmod 4 \quad (5)$$

由式(4)和式(5)可见, 加密变换与解密变换规则完全一样, 仅密钥使用方式不同, 这正好符合现代分组密码算法设计的相应要求. 而且, 实际密钥空间 $K_1 = Z_2^2$ 中的每个密钥都是同等可用的, 不

存在弱密钥问题.

2.2 基本实际密码系统 2 ($M_2 = C_2 = Z_2^3$, $K_2 = Z_2^3$, E_2, D_2): 实际密钥空间 K_2 由 3 bit 组成

当 $K_2 = Z_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$ 时, 选择两个正交拉丁方 $\{L_1, L_2\}$ 作为理论密钥空间, 设计与实际密钥空间 $K_2 = Z_2^3$ 相应的加解密变换. 参照可逆变换 $T_1, T_2, \dots, T_8$ 及其逆变换的代数式, 将基本实际密码系统 ($M_2 = C_2 = Z_2^3$, $K_2 = Z_2^3$, E_2, D_2) 设计为:

1) 加密变换 E_2 : 对任一 2 bit 明文 $m = m_1 m_2 \in Z_2^2$ 和任意 3 bit 密钥 $k = k_1 k_2 k_3 \in Z_2^3$, 其中, $m_1, m_2, k_1, k_2, k_3 \in Z_2$, 将 E_2 设计为

$$c = E_2(k, m) = [(\bar{k}_1 \wedge \bar{k}_2 \wedge \bar{k}_3) \times T_1(m) + (\bar{k}_1 \wedge \bar{k}_2 \wedge k_3) \times T_2(m) + (\bar{k}_1 \wedge k_2 \wedge \bar{k}_3) \times T_3(m) + (\bar{k}_1 \wedge k_2 \wedge k_3) \times T_4(m) + (k_1 \wedge \bar{k}_2 \wedge \bar{k}_3) \times T_5(m) + (k_1 \wedge \bar{k}_2 \wedge k_3) \times T_6(m) + (k_1 \wedge k_2 \wedge \bar{k}_3) \times T_7(m) + (k_1 \wedge k_2 \wedge k_3) \times T_8(m)] \bmod 4 \quad (6)$$

2) 解密变换 D_2 : 对任一 2 bit 密文 $c = c_1 c_2 \in Z_2^2$ 和任意 3 bit 密钥 $k = k_1 k_2 k_3 \in Z_2^3$, 其中, $c_1, c_2, k_1, k_2, k_3 \in Z_2$, 将 D_2 设计为

$$m = D_2(k, c) = [(\bar{k}_1 \wedge \bar{k}_2 \wedge \bar{k}_3) \times T_1^{-1}(c) + (\bar{k}_1 \wedge \bar{k}_2 \wedge k_3) \times T_2^{-1}(c) + (\bar{k}_1 \wedge k_2 \wedge \bar{k}_3) \times T_3^{-1}(c) + (\bar{k}_1 \wedge k_2 \wedge k_3) \times T_4^{-1}(c) + (k_1 \wedge \bar{k}_2 \wedge \bar{k}_3) \times T_5^{-1}(c) + (k_1 \wedge \bar{k}_2 \wedge k_3) \times T_6^{-1}(c) + (k_1 \wedge k_2 \wedge \bar{k}_3) \times T_7^{-1}(c) + (k_1 \wedge k_2 \wedge k_3) \times T_8^{-1}(c)] \bmod 4 = [(\bar{k}_1 \wedge \bar{k}_2 \wedge \bar{k}_3) \times T_1(c) + (\bar{k}_1 \wedge \bar{k}_2 \wedge k_3) \times T_2(c) + (\bar{k}_1 \wedge k_2 \wedge \bar{k}_3) \times T_3(c) + (\bar{k}_1 \wedge k_2 \wedge k_3) \times T_4(c) + (k_1 \wedge \bar{k}_2 \wedge \bar{k}_3) \times T_5(c) + (k_1 \wedge \bar{k}_2 \wedge k_3) \times T_6(c) + (k_1 \wedge k_2 \wedge \bar{k}_3) \times T_7(c) + (k_1 \wedge k_2 \wedge k_3) \times T_8(c)] \bmod 4 \quad (7)$$

由式(6)和式(7)可见, 加密变换与解密变换规则一样, 仅密钥使用方式不同且实际密钥空间 $K_2 = Z_2^3$ 中每个密钥都是同等可用的.

2.3 实际基本密码系统 $3(M_3 = C_3 = Z_2^2, K_3 = Z_2^4, E_3, D_3)$: 实际密钥空间 K_3 由 4 bit 组成

当 $K_3 = Z_2^4$ 时, 选择在两两正交拉丁方组 $\{L_1, L_2, L_3\}$ 中增加第 2 个拉丁方 L_2 所得到的拉丁方组 $\{L_1, L_2, L_3, L_2\}$ 作为理论密钥变换空间, 设计相应的实际密钥空间及其相应的加解密变换. 直观上, 利用这种有重复的密钥变换方式可在形式上避免密钥空间存在冗余的问题.

由文献[6]可知, 若仅利用式(1)的正交拉丁方组 $\{L_1, L_2, L_3\}$ 设计基本理论密钥空间, 则有密钥 12 个, 因而不能将 Z_2^4 中的每个 bit 向量都用来设计密钥空间, 此即冗余问题. 为消除这种冗余, 重复利用拉丁方 L_2 设计 4 bit 实际密钥空间能从形式上使 Z_2^4 中每个 bit 向量都用于设计密钥变换, 而这种做法是有理论基础的. 理论上, 文献[6]定理 1 所要求的基本密码系统是一个正交拉丁方组, 且由同一个拉丁方所决定的全部可逆变换被等概率使用, 但不同拉丁方所决定的两个部分可逆变换组可被不等概率使用. 这样, 在理想情形下, 对于利用 $\{L_1, L_2, L_3, L_2\}$ 所设计的基本密码系统, 当其应

用密钥单元序列设计为独立均匀无限随机序列时, 所设计的保密通信系统实际上等价于利用 $\{L_1, L_2, L_3\}$ 所设计的基本密码系统, 且其应用密钥单元序列为某种独立的特定非均匀无限随机序列. 其中, L_1 和 L_3 所决定的密钥变换是等概率使用, 且以其 2 倍概率利用 L_2 所决定的密钥变换组. 因此, 利用 $\{L_1, L_2, L_3, L_2\}$ 设计相应的 4 bit 实际密钥空间在理论上符合定理 1. 这种有重复的设计方式还可推广为一般情形, 即对任意给定的基本密码系统, 理论上可通过调整相应的应用系统中密钥流序列的统计特性, 就可使利用无重复和有重复基本密码系统的两种保密通信的整体效果相同. 这无疑会提高实际流密码算法设计的灵活性.

参照由 $\{L_1, L_2, L_3, L_2\}$ 所确定的 16 个可逆变换的代数式, 将密钥长度为 4 bit 的实际基本密码系统 $(M_3 = C_3 = Z_2^2, K_3 = Z_2^4, E_3, D_3)$ 设计为:

1) 加密函数 E_3 : 对任一 2 bit 明文 $m = m_1 m_2 \in Z_2^2$ 和任意 4 bit 密钥 $k = k_1 k_2 k_3 k_4 \in Z_2^4$, 其中, $m_1, m_2, k_1, k_2, k_3, k_4 \in Z_2$, 可利用如下统一代数式将加密变换 $c = E_3(k, m)$ 设计为

$$\begin{aligned} c = & [\bar{k}_1 \times T_1(m) + \bar{k}_2 \times T_2(m) + \bar{k}_3 \times T_3(m) + \bar{k}_4 \times T_4(m) + \bar{k}_5 \times T_5(m) + \bar{k}_6 \times T_6(m) + \\ & \bar{k}_7 \times T_7(m) + \bar{k}_8 \times T_8(m) + \bar{k}_9 \times T_9(m) + \bar{k}_{10} \times T_{10}(m) + \bar{k}_{11} \times T_{11}(m) + \bar{k}_{12} \times T_{12}(m) + \\ & \bar{k}_{13} \times T_5(m) + \bar{k}_{14} \times T_6(m) + \bar{k}_{15} \times T_7(m) + \bar{k}_{16} \times T_8(m)] \bmod 4 = \\ & \bar{k}_1 \times T_1(m) + \bar{k}_2 \times T_2(m) + \bar{k}_3 \times T_3(m) + \bar{k}_4 \times T_4(m) + (\bar{k}_5 + \bar{k}_{13}) \times T_5(m) + \\ & (\bar{k}_6 + \bar{k}_{14}) \times T_6(m) + (\bar{k}_7 + \bar{k}_{15}) \times T_7(m) + (\bar{k}_8 + \bar{k}_{16}) \times T_8(m) + \bar{k}_9 \times T_9(m) + \\ & \bar{k}_{10} \times T_{10}(m) + \bar{k}_{11} \times T_{11}(m) + \bar{k}_{12} \times T_{12}(m)] \bmod 4 \end{aligned} \quad (8)$$

其中, $\bar{k}_1 = (\bar{k}_1 \wedge \bar{k}_2 \wedge \bar{k}_3 \wedge \bar{k}_4)$; $\bar{k}_2 = (\bar{k}_1 \wedge \bar{k}_2 \wedge \bar{k}_3 \wedge k_4)$; $\bar{k}_3 = (\bar{k}_1 \wedge \bar{k}_2 \wedge k_3 \wedge \bar{k}_4)$; $\bar{k}_4 = (\bar{k}_1 \wedge \bar{k}_2 \wedge k_3 \wedge k_4)$; $\bar{k}_5 = (\bar{k}_1 \wedge k_2 \wedge \bar{k}_3 \wedge \bar{k}_4)$; $\bar{k}_6 = (\bar{k}_1 \wedge k_2 \wedge \bar{k}_3 \wedge k_4)$; $\bar{k}_7 = (\bar{k}_1 \wedge k_2 \wedge k_3 \wedge \bar{k}_4)$; $\bar{k}_8 = (\bar{k}_1 \wedge k_2 \wedge k_3 \wedge k_4)$; $\bar{k}_9 = (k_1 \wedge \bar{k}_2 \wedge \bar{k}_3 \wedge \bar{k}_4)$; $\bar{k}_{10} = (k_1 \wedge \bar{k}_2 \wedge \bar{k}_3 \wedge k_4)$; $\bar{k}_{11} = (k_1 \wedge \bar{k}_2 \wedge k_3 \wedge \bar{k}_4)$; $\bar{k}_{12} = (k_1 \wedge \bar{k}_2 \wedge k_3 \wedge k_4)$; $\bar{k}_{13} = (k_1 \wedge k_2 \wedge \bar{k}_3 \wedge \bar{k}_4)$; $\bar{k}_{14} = (k_1 \wedge k_2 \wedge \bar{k}_3 \wedge k_4)$; $\bar{k}_{15} = (k_1 \wedge k_2 \wedge k_3 \wedge \bar{k}_4)$; $\bar{k}_{16} = (k_1 \wedge k_2 \wedge k_3 \wedge k_4)$.

由式(8)可见, 只要调整好各自的应用密钥流序列的统计特性, 利用有重复和无重复拉丁方组所设计的基本密码系统构造出的两种保密通信系统就会是等价的.

2) 解密函数 D_3 : 对任一 2 bit 密文 $c = c_1 c_2 \in Z_2^2$ 和任意 4 bit 密钥 $k = k_1 k_2 k_3 k_4 \in Z_2^4$, 其中, $c_1, c_2, k_1, k_2, k_3, k_4 \in Z_2$, 可将解密变换 $m = D_3(k, c)$ 设计为

$$\begin{aligned} m = & [(\bar{k}_7 + \bar{k}_{15}) \times T_1(c) + (\bar{k}_6 + \bar{k}_{14}) \times T_2(c) + \\ & (\bar{k}_8 + \bar{k}_{16}) \times T_3(c) + (\bar{k}_5 + \bar{k}_{13}) \times T_4(c) + \\ & \bar{k}_4 \times T_5(c) + \bar{k}_2 \times T_6(c) + \bar{k}_1 \times T_7(c) + \end{aligned}$$

$$\begin{aligned} & \bar{k}_3 \times T_8(c) + \bar{k}_9 \times T_9(c) + \bar{k}_{10} \times T_{10}(c) + \\ & \bar{k}_{12} \times T_{11}(c) + \bar{k}_{11} \times T_{12}(c)] \bmod 4 \end{aligned} \quad (9)$$

由式(8)和式(9)可见, 加密变换规则与解密变换规则一样, 仅密钥使用方式不同. 而且, 实际密钥空间 $K_3 = Z_2^4$ 中的每个密钥单元都可用, 其中 4 个密钥是另外 8 个密钥被使用频率的 1 倍.

上述 3 种 2 bit (明密文空间) 基本密码系统都是非线性的^[6], 而重复利用 2 次常见的逐个 bit 异或运算所设计的 2 bit 基本密码系统是线性的, 因而可认为利用这 3 种非线性新基本密码系统设计流密码算法将完全不同于现有常见的流密码算法,

且(加解密或被攻击或破解的)计算量会更大。

为说明上述基本密码系统能用于设计完整的流密码算法,结合 JK 触发器所产生的密钥流序列设计了一个简单流密码算法,对 1 个短英文文本文件进行加密,得到的加密文件为乱码。算法代码、原文件及加密文件请扫描论文末页右下角二维码查看图 S1、S2 和 S3。

结 语

本研究基于文献[6],利用 1 个 4 阶正交拉丁方组设计 3 种不同的 4 元或 2 bit(明密文空间)非线性基本密码系统。本研究具有以下特点:

1) 在现有流密码算法中,通常采用标量置乱编码方式的模 2 加法线性基本密码系统,它等价于利用 2 阶正交拉丁方设计基本密码系统,该方法的单一性决定了现有基本密码系统研究缺乏技巧性和丰富性。本研究利用矢量置乱编码方式的 4 阶正交拉丁方组设计基本密码系统,高阶正交拉丁方组及其代数式构造灵活多样,丰富了基本密码系统的设计方法。

2) 所提出 4 阶正交拉丁方组的非统一代数计算式构造方法,有利于推广到更高阶拉丁方组的构造上。通过对拉丁方组所决定的理论密钥变换进行统一的代数式设计,建立 3 种基本密码系统的实际模型,可用于新的序列密码算法设计。这种综合考虑基本密码系统理论模型和实际模型的设计方法,可为现有序列密码算法设计提供参考。利用理论密钥变换更利于分析密钥变换的性能,而利用实际密钥及其加密变换更利于在计算机实现。因此,理论与实际密码模型并重的设计方法对单钥密码算法设计都具有启发意义。

综上,4 阶拉丁方组的构造方法对高阶拉丁方组的构造具有一定的指导作用,有利于进一步研究设计基本密码系统及其流密码系统。

基金项目:国家自然科学基金资助项目(61070252)

作者简介:田传俊(1964—),深圳大学教授。研究方向:伪随机性理论和密码算法。E-mail: tiancj@szu.edu.cn

引 文:田传俊.基于 4 阶正交拉丁方组实际基本密码系统设计[J].深圳大学学报理工版,2020,37(3):251-256.

参考文献 / References:

- [1] SHANNON C E. Communication theory of secrecy system [J]. Bell System Technical Journal, 1949, 28: 656-715.

<http://journal.szu.edu.cn>

- [2] 章照止.现代密码学基础[M].北京:北京邮电大学出版社,2004.

ZHANG Zhaozhi. Fundamentals of modern cryptography [M]. Beijing: Beijing University of Posts and Telecommunications Press, 2004. (in Chinese)

- [3] 丁存生,肖国镇.流密码学及其应用[M].北京:国防工业出版社,1994.

DING Cunsheng, XIAO Guozhen. Stream cryptography and its application [M]. Beijing: National Defense Industry Press, 1994. (in Chinese)

- [4] SUDEEPTHI G, DHAVALA S K, KUMAR G R. Perfect secrecy designs for contracted rule mining [J]. International Journal of Advanced Research in Science and Technology, 2015, 4(3), 348-352.

- [5] 亢保元,王育明.完善保密密码体制的条件与设计[J].通信学报,2004,25(2):168-173.

HANG Baoyuan, WANG Yuming. On the condition and design of perfect secrecy cryptosystem [J]. Journal of China Institute of Communications, 2004, 25(2): 168-173. (in Chinese)

- [6] 田传俊.密钥非均匀分布的完善保密通信系统[J].通信学报,2018,39(11):1-9.

TIAN Chuanjun. Perfect secrecy cryptosystem with nonuniform distribution of keys [J]. Journal on Communications, 2018, 39(11): 1-9. (in Chinese)

- [7] 田传俊.频率不相关性及其在单钥密码系统中的应用[J].深圳大学学报理工版,2015,32(1):32-39.

TIAN Chuanjun. Frequency irrelevance and its applications in one-key cryptosystems [J]. Journal of Shenzhen University Science and Engineering, 2015, 32(1): 32-39. (in Chinese)

- [8] 张 斌,徐 超,冯登国.流密码的设计与分析:回顾、现状与展望[J].密码学报,2016,3(6):527-545.

ZHANG Bin, XU Chao, FENG Dengguo. Design and analysis of stream ciphers: past, present and future directions [J]. Journal of Cryptologic Research, 2016, 3(6): 527-545. (in Chinese)

- [9] ZUC 算法研制组. ZUC-256 流密码算法[J].密码学报,2018,5(2):167-179.

DESIGN TEAM. ZUC-256 stream cipher [J]. Journal of Cryptologic Research, 2018, 5(2): 167-179. (in Chinese)

【中文责编:英 子;英文责编:木 柯】

补充材料