密钥非均匀分布的完善保密通信系统

田传俊
（深圳大学信息工程学院，广东 深圳 518060）

摘 要：提出了理论上更加严格的无限完善保密性和随机“一次一密”保密通信系统的概念，并将保密通信设计过程划分为基本密码系统设计及其应用设计两个阶段。首先研究了利用正交拉丁方组设计基本密码系统的问题，并举例说明了其非线性加密变换的设计方法；然后讨论了利用一类非均匀分布的随机方法设计应用过程中密钥序列的问题，并在理论上严格证明了基于所设计的基本密码系统的随机“一次一密”无限保密通信系统具有完善保密性。这一成果推广了当前常见的基于“模加法密码系统”的随机“一次一密”完善保密通信系统，因而可将其作为序列密码算法设计的一种更广泛的理想模拟原型。由于所能设计的基本密码系统的数量远超过现有常用方法所能设计的基本密码系统的数量，因此，所得结果对当前序列密码算法的主流设计方法是一种有效的补充与完善。

关键词：单钥密码系统；完善保密性；非线性基本密码系统；一次一密系统；正交拉丁方组
中图分类号：TN918
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018234

Perfect secrecy cryptosystem with nonuniform distribution of keys

TIAN Chuanjun
College of Information Engineering, Shenzhen University, Shenzhen 518060, China

Abstract: More strictly mathematical concepts of infinite perfect secrecy and random “one-time pad” cryptosystem in theory were presented, and the whole secure communication system was divided into two stages: design of a basic cryptosystem and one of its applications. How to design a basic cryptosystem by using a group of orthogonal Latin squares was first studied and an example to illustrate how to design nonlinear encryption transformations for a basic cryptosystem was given. Then, how to design the sequence of keys by using random method with nonuniform distribution was discussed, and it was strictly proven in theory that the infinite random “one-time pad” cryptosystem based on the designed basic cryptosystem was of perfect secrecy. Since the obtained result generalizes the existing one for random “one-time pad” cryptosystem to be perfect by using a basic cryptosystem with modulo addition, it may be used as a wider ideal simulated prototype to design stream cipher algorithms. Since the number of basic cryptosystems that can be designed is much more than one of the common basic cryptosystems with modulo addition, the obtained result is effective supplement and perfection to mainstream design method for the current stream cryptosystems.

Key words: single key cryptosystem, perfect secrecy, nonlinear basic cryptosystem, one-time pad cryptosystem, orthogonal Latin square

1 引言

随着计算机科学与技术的发展，信息安全已成为当今科学研究的重大课题之一。密码学是信息安全领域中一门重要的基础理论课程。在密码学理论的发展过程中，Shannon[1]曾做出杰出贡献，他于1949 年创立了基于信息论的保密通信理论，以概率统计的观点对消息源、密钥源、接收和截获消息进

收稿日期：2018–01–11；**修回日期**：2018–06–30
基金项目：国家自然科学基金资助项目（No.61070252）
Foundation Item: The National Natural Science Foundation of China (No.61070252)

行了数学描述和分析，阐明了密码系统、完善保密性、理论安全性和实际安全性等一系列重要概念，从此宣告了科学的密码学信息理论时代的到来[2]。现代密码学理论将密码系统或算法分为单钥密码系统和双钥密码系统，其中，单钥密码系统又可分为序列（或流）密码系统和分组密码系统。

人们普遍认为，Shannon 保密通信理论诞生后在 1949—1976 年间基本上停滞不前。1976 年，Diffie 等[3]发表的论文《密码编码学新方向》引起了密码学理论及其应用上的又一次革命，影响并引领了之后的密码学研究的发展方向，极大地促进了计算复杂性理论和保密通信理论及其应用的发展。可以说这次革命极大地促进了 Shannon 理论中与实际安全性相关的保密通信理论的发展，但对理论安全性相关的保密通信理论的影响有限，因而保密通信理论中与理论安全性相关的理论及其应用研究还有待进一步的发展和完善。

参照微积分理论及其成功应用的经验，可以说理论研究的一个主要特点是需要研究无限精度的理想情形，而实际应用研究的主要特点是研究以理想情形为目标的有限精度的现实情形。受此启发，首先需要明确如何描述保密通信系统的理想情形与实际应用情形。Shannon 在文献[1]中指出保密系统中被加密的对象是从一个有限符号集中取出的一串离散信号，并构成一个随机序列或随机过程。这样，在考虑所有可能的一列被加密的离散符号信号时，自然会想到将大量被加密的明文信号当作一个理想的无限随机序列（即含无限多个离散符号），因而理论上需要研究“无限”保密通信的理想情形。毫无疑问，研究“无限”保密通信情形会比有限保密通信情形更加广泛、全面与深刻。另一方面，在实际应用中，所设计的保密系统只能是有限长度的，且需要将该有限长度的保密系统用于任意长度的保密通信之中。因此，为了便于实际应用，只能先设计出某个固定长度的保密系统（可称为基本保密系统或基本密码系统），然后再反复利用该基本密码系统多次地加密这个固定长度的明文信号即可实现任何长度的保密通信。下文中所说的无限保密通信是指利用一个基本密码系统中无限多个明文进行的保密通信。

为了便于理论研究和实际应用，基于上述分析和现有文献，可以将整个保密通信系统的设计过程划分为两个阶段：1) 基本密码系统设计；2) 将基本密码系统应用于所有可能的保密通信的设计，即应用系统设计。基于这一观点，下面先利用正交拉丁方组来设计一类基本密码系统，之后再讨论所设计的基本密码系统的一种理想应用设计。

需要说明的是，文献[1]及其后续文献[2-14]有关完善保密通信系统的研究基本可归属于有限保密通信系统的研究范畴。这可能是由于现有关于完善保密通信的研究文献都只关注实际上所有可能的保密通信问题，但却很少关注理论上所有可能的保密通信问题而造成的。在理论上，通常会认为无限情形是有限情形的理想化推广，其研究方法更加严格与深刻，因而本文研究的无限保密通信系统是新颖和有意义的。

2 正交拉丁方组

下面先介绍正交矩阵和正交拉丁方组的相关知识[15-19]。

设 n 阶方阵 $\boldsymbol{A}=(a_{ij})_{n\times n}$ 和 $\boldsymbol{B}=(b_{ij})_{n\times n}$ 都是由数字 $0,1,\cdots,n-1$ 构成的，且

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

其中，$a_{ij},b_{ij}\in\{0,1,\cdots,n-1\}$，并记

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

定义 1 设 $n\in\{2,3,4,5,\cdots\}$。如果 $Z_n=\{0,1,\cdots,n-1\}$ 上所有不同的数字在 n 阶方阵 $\boldsymbol{L}$ 的每行和每列中都出现，则称 $\boldsymbol{L}$ 为 n 阶拉丁方。

定义 2 如果 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 都是由 $0,1,\cdots,n-1$ 构成的 n 阶方阵，且 $(\boldsymbol{A},\boldsymbol{B})$ 的 n^2 个元素组成的集合等于 $\{(i,j)\,|\,i,j=0,1,\cdots,n-1\}=Z_n^2$，则称 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是正交的，也称 $\{\boldsymbol{A},\boldsymbol{B}\}$ 为正交对。特别地，如果 $k(k\geqslant 2)$ 个拉丁方 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_k$ 两两正交，则称 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_k$ 为正交拉丁方组。

为了叙述方便，将由一个拉丁方组成的集合也称为正交拉丁方组。

关于正交拉丁方组的存在性和数量，有如下常见结果。

引理 1　设 p 是素数，r 是正整数，且 $n=p^r>2$，则存在 $n-1$ 个两两正交的 n 阶拉丁方组。

例 1　对任一整数 $n>1$，设 n 阶方阵为

$$\boldsymbol{A}=\begin{bmatrix}0 & 1 & \cdots & n-1\\ 0 & 1 & \cdots & n-1\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 1 & \cdots & n-1\end{bmatrix},\quad \boldsymbol{B}=\begin{bmatrix}0 & 1 & \cdots & n-1\\ 1 & 2 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ n-1 & 0 & \cdots & n-2\end{bmatrix} \tag{3}$$

不难验证 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是两个相互正交的 n 阶矩阵。将 $\boldsymbol{A}$ 称为 n 阶标准或规范矩阵。为了方便，下面将有限集合到其自身上的可逆变换称为置换。显然，$\boldsymbol{B}$ 的每一行都与 $\boldsymbol{A}$ 的相应一行互为置换。

3　完善密码系统

关于保密系统的概念，Shannon 在文献[1]中曾给出了两种略有不同的定义，分别介绍如下。

第一种定义：在文献[1]的序言中 Shannon 将保密系统定义为从明文集 M 到密文集 C 的一组可逆变换 T。根据这种定义，文献[20]将保密系统记为 (M,T,C)，并称之为理论模型或理论系统，T^{-1} 为理论密钥（变换）集 T 的逆变换集。通常需要将 T 和 T^{-1} 转化为方便实际应用的集合 K 和加密变换 E 与解密变换 D 来实现。因此，保密系统常表示为 (M,K,C,E,D)，称之为实际模型或综合模型，K 为实际密钥集。同一个理论模型可利用多种不同形式的实际模型来实现，因而保密系统的理论模型是实际模型的基础。

第二种定义：在文献[1]的第一部分 Shannon 又将保密系统定义为从明文集到密文集的一组可逆变换，且该可逆变换集或密钥集具有一定的概率分布。显然，第二种定义是在第一种定义基础上增加了密钥变换集要服从某个随机分布这一新要素。可进行如下直观分析：为了防止实际保密通信受到攻击，密钥随机性应该是由将大量保密密钥分配给不同用户而产生的，而用户群进行保密通信的方式或频繁程度会决定密钥集所具有的随机分布类型。

综合分析可得，第一种定义更适合于通用的基本密码系统的设计场合；而第二种定义更适合于将“基本密码系统”大量应用于实际保密通信的场合。

将整个保密通信系统设计过程分为两个阶段是指，首先设计基本密码系统 (M,T,C) 或 (M,K,C,E,D)，然后设计其实际应用过程。将 M 与 T 分别称为（基本）明文空间与理论密钥空间，并将从中取出的 n 个明文或密钥称为长度为 n 的（明文等）单元序列，$n=1,2,\cdots$。当考虑实际有限保密通信时，需要研究基本密码系统 (M,T,C) 的某个有限重密码系统 (M^r,T^r,C^r) 的相关问题，其中，$M^r=M\times M^{r-1}$，r 是正整数。称 (M^r,T^r,C^r) 或 (M^r,K^r,C^r,E^r,D^r) 为原基本密码系统 (M,T,C) 或 (M,K,C,E,D) 的 r 重基本密码系统，统称为多重密码系统。

在利用一个基本密码系统 (M,T,C) 或 (M,K,C,E,D) 进行保密通信的应用过程中，Shannon 假设明文的选取规则是随机的，因而需要从明文空间 M 中多次随机选取明文（基本）单元从而得到一列明文（单元）随机序列 $M_1,M_2,\cdots$。密文空间 C 和密钥空间 K 或 T 也有类似的情况。本文将从 M、K 和 C 中随机选取的任一单元仍然表示为 M、K 和 C，将一次保密通信中具体选中的明文、密钥和密文单元分别设为 m、k 或 t 和 c，则任一单元的加密可表示为

$$C=E(K,M)=E_K(M)=T(M) \tag{4}$$

$$c=E(k,m)=E_k(m)=t(m) \tag{5}$$

任一单元的解密可表示为

$$M=D(K,C)=D_K(C)=T^{-1}(C) \tag{6}$$

$$m=D(k,c)=D_k(c)=t^{-1}(c) \tag{7}$$

根据计算机密码学的应用现状，设明文空间是由所有不同的 n bit 二进制序列所组成的，即 $M=\{0\cdots00,0\cdots01,\cdots,1\cdots11\}=Z_2^n$。在现有的理论研究中，可利用十进制数将该明文空间简单地表示为 $M=\{0,1,\cdots,u-1\}=Z_u$ 和 $u=2^n$，同样地，密文空间 C 和密钥空间 K 也有类似的表示。

在文献[1]中，Shannon 假设所有密文都有可能被窃取。在只讨论唯密文攻击时，明文单元和密钥单元序列都应该是保密的，但理论上所有相应的密文单元序列不是保密的。在考虑实际应用有限保密通信时，可利用 $\overline{M}$、$\overline{K}$ 和 $\overline{C}$ 表示某一段明文、密钥和密文单元序列。

保密通信的核心问题是其安全性，为了描述保密通信的安全性，Shannon 曾提出了完善保密性概念[1-3]，它可描述所截获的密文对攻击某段明文无

任何帮助。现有文献都只是研究了有限保密通信系统的完善保密性问题。因此，参照文献[1-14]，可按照如下方式给出这种“有限”完善保密性概念。

定义 3 在利用一个基本密码系统 (M, T, C) 进行保密通信时，设随机选取的某一段明文为 $\bar{M}$，相关密文为 $\bar{C}$，即存在某一整数 $r>0$，使得随机选取的任意明文 $\bar{M}\in M^r$，且相关的任意密文 $\bar{C}\in C^r$。如果互信息 $I(\bar{M},\bar{C})=0$ 或 $\bar{M}$ 与 $\bar{C}$ 相互独立，则称该保密系统为完善的。

根据文献[1,2,4-6]，“有限”完善保密系统是存在的，公认的完善保密系统是随机“一次一密”（有限）保密系统。因此，有限完善保密通信来源于将一个基本密码系统应用于某个有限长度的所有可能保密通信。但是，本文所讨论的理想保密通信是所用可能的无限保密通信，因而任何一段有限明文和密文都会被认为是从无限长的明文和密文单元序列中所截取的。这样，需要将定义 3 所描述的“有限完善保密性”推广为“无限完善保密性”。因此，可以将无限完善保密性和随机“一次一密”保密系统做出如下严格的数学表述。

设 (M,T,C) 或 (M,K,C,E,D) 是一个基本密码系统，在所有可能的无限保密通信中，从明文源中依次随机选取明文会得到一个无限长明文单元随机序列 $M_1,M_2,\cdots$。设对每个单元 $M_i\in M$ 加密所用的密钥单元 T_i 或 K_i 也是随机的，且利用密钥单元随机序列 $T_1,T_2,\cdots$ 或 $K_1,K_2,\cdots$ 依次加密明文单元会得到密文单元随机序列 $C_1,C_2,\cdots$，其中，对任意 $i=1,2,\cdots$，$C_i=T_i(M_i)=E_{K_i}(M_i)$。这样所描述的保密通信系统可认为是随机“一次一密”无限保密通信系统，它是相应有限系统的推广。

定义 4 在利用一个基本密码系统 (M,T,C) 进行所有可能的无限保密通信过程中，设所有可能的明文单元和密文单元序列都是无限随机序列。如果该无限明文单元随机序列与相应的密文单元随机序列是相互独立的，即对任意整数 $r>0$，随机选取的明文序列 $M_1,M_2,\cdots,M_r\in M^r$ 和相应密文随机序列 $C_1,C_2,\cdots,C_r\in C^r$ 相互独立，则将该无限保密通信系统或密码系统称为完善的。

显然，定义 4 是将定义 3 中的某个有限长度加强为任意长度的明文序列与密文序列之间的相互独立，或者形象地说，定义 4 是将定义 3 所描述的“有限完善性”理想化为“无限完善性”了，因而定义 4 的完善性更加严格。因此，下面将要证明的无限完善保密通信系统比现有有限完善保密系统更加严格，能保证该无限完善保密通信系统也具有有限完善保密性。

4 基于正交拉丁方组的完善保密通信系统设计

4.1 基本密码系统的设计

将要设计的基本密码系统记为 (M,T,C) 或 (M,K,C,E,D)。选定一个整数 $n\geqslant 2$，将基本明文和密文空间设计为 $M=C=Z_n=\{0,1,\cdots,n-1\}$，且基本密钥空间 T 或 K 中不同密钥单元的个数正好为 n 的正整数倍。特别地，在计算机保密通信中，明文单元常为 r bit，此时 $n=2^r$。由于加密变换完全决定了解密变换，因此，在理论上不关注实现难度的情况下，只需设计好加密变换即可。需要说明：利用加密变换来确定解密变换有时可能会非常复杂，但可以在算法实际模型的具体设计中解决这个问题。

当 M 和 C 确定后，需要研究 T 或 K 的设计问题。将正交拉丁方组作为可逆的密钥置换组时，全体明文与密文单元对的分布会非常均匀，这会导致与每个密文单元可能配对的明文单元的“不确定性”是最大的。因此，下面考虑利用一个两两正交拉丁方组来设计 T 的方法。

设 n 阶正交拉丁方组为 $\{\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_q\}$。由引理 1 可知，对任一素数 p 和正整数 r，当 $n=p^r>2$ 时，$\{\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_q\}$ 所包含的矩阵个数至少为 $q=n-1$。设 $\boldsymbol{A}$ 是如式(3)所示的 n 阶标准矩阵，则 $\boldsymbol{A}$ 和 $\boldsymbol{A}_i(i=1,\cdots,q)$ 的每一行都可看成是明文或密文空间，因此每个对应行所决定的置换都可作为加密变换。基于此，利用 $\{\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_q\}$ 对 (M,T,C) 中的理论密钥或加密变换空间 T 可进行如下的设计。

将每个加密变换设计为 $b_{ij}^{(s)}=\tilde{T}_{si}(a_{ij})=\tilde{T}_{si}(j-1)$，即对任一明文单元 $a_{ij}\in\boldsymbol{A}=(a_{ij}=j-1)$ 加密后所对应的密文单元为 $b_{ij}^{(s)}\in\boldsymbol{A}_s=(b_{ij}^{(s)})$，对每个 $i,j\in\{1,2,\cdots,n\}$ 和 $s\in\{1,2,\cdots,q\}$，所设计的理论密钥空间为 $T=\{\tilde{T}_{11},\cdots,\tilde{T}_{1n},\tilde{T}_{21},\cdots,\tilde{T}_{2n},\cdots,\tilde{T}_{q1},\cdots,\tilde{T}_{qn}\}$。

上面设计的理论模型 (M,T,C) 所确定的实际模型 (M,K,C,E,D) 的设计方法应该存在且不唯一。

4.2　基本密码系统的应用设计

将某个基本密码系统用于大量实际保密通信的过程中，所遇到的明文千差万别，因此难以完全控制明文的统计特性。在整个保密通信系统的应用系统设计中，本文主要考虑密钥单元序列的设计问题。由于完善保密性能保证密文单元序列不包含明文单元序列的任何信息，利用密文序列来攻击明文几乎没有作用，因此，常将其当成一种理想安全的保密通信系统。这样，在只考虑系统安全性且暂时不考虑密钥分配难度的情况下，为了保证所有可能的保密通信具有完善性，可将选取的密钥序列设计为某种不受明文影响的理想随机序列，得到定理 1。

定理 1　对于上述利用 q 个正交拉丁方组 $\boldsymbol{A}_1, \boldsymbol{A}_2,\cdots,\boldsymbol{A}_q$ 设计的加密变换规则所确定的基本密码系统 $(M=C=Z_n,T)$ 或 $(M=C=Z_n,K,E,D)$，其中，$q=2,3,\cdots$，$|T|$或$|K|=nq$，设明文单元序列是一个随机序列，$\{\tilde{T}_{i1},\tilde{T}_{i2},\cdots,\tilde{T}_{in}\}$ 是由第 i 个拉丁方 $\boldsymbol{A}_i$ 所决定的一组子理论密钥变换，对任意 $i=1,2,\cdots,q$，概率分布 $\{p_1,p_2,\cdots,p_q\}$ 是一组非负实数，且 $p_1+p_2+\cdots+p_q=1$。如果对明文单元随机序列依次加密所选用的密钥单元序列是一列独立随机序列，子密钥组 $\{\tilde{T}_{i1},\tilde{T}_{i2},\cdots,\tilde{T}_{in}\}$ 中每个密钥是以相同的概率 $\dfrac{p_i}{n}$ 被使用的，对任意 $i(i=1,2,\cdots,q)$，且明文单元随机序列与密钥单元随机序列是相互独立的，则该无限保密通信系统是完善的。

证明　设明文单元序列为 $M_1,M_2,\cdots$，所用密钥单元序列为 $T_1,T_2,\cdots$ 或 $K_1,K_2,\cdots$，且依次加密所得的密文单元随机序列为 $C_1,C_2,\cdots$，则 $C_j=E(K_j,M_j)=T_j(M_j)$，对任意 $T_j\in T$ 和 $K_j\in K$，对任意 $j(j=1,2,\cdots)$，且 $T=\{\tilde{T}_{11},\cdots,\tilde{T}_{1n},\cdots,\tilde{T}_{q1},\cdots,\tilde{T}_{qn}\}$ 等。设 $\tilde{k}_{ir}$ 是与理论密钥 $\tilde{T}_{ir}$ 相互唯一对应的实际密钥，对任意 $i(i=1,2,\cdots,q)$ 和 $r(r=1,2,\cdots,n)$，其中，$K=\{\tilde{k}_{11},\cdots,\ \tilde{k}_{1n},\cdots,\tilde{k}_{q1},\cdots,\tilde{k}_{qn}\}$ 与 T 相互唯一确定。下面利用实际密钥随机序列 $K_1,K_2,\cdots$ 给出证明，这不会到影响证明的本质。

设 $\tilde{T}_1=\{\tilde{T}_{11},\tilde{T}_{12},\cdots,\tilde{T}_{1n}\},\tilde{T}_2=\{\tilde{T}_{21},\tilde{T}_{22},\cdots,\tilde{T}_{2n}\},\cdots,\tilde{T}_q=\{\tilde{T}_{q1},\tilde{T}_{q2},\cdots,\tilde{T}_{qn}\}$，且与它们相互唯一对应的实际密钥组分别为 $\tilde{K}_1=\{\tilde{k}_{11},\tilde{k}_{12},\cdots,\tilde{k}_{1n}\},\tilde{K}_2=\{\tilde{k}_{21},\tilde{k}_{22},\cdots,\tilde{k}_{2n}\},\cdots,\tilde{K}_q=\{\tilde{k}_{q1},\tilde{k}_{q2},\cdots,\tilde{k}_{qn}\}$，则对任意 $j(j=1,2,\cdots)$，$i(i=1,2,\cdots,q)$ 和 $r(r=1,2,\cdots,n)$，有 $P\{K_j=\tilde{k}_{ir}\}=P\{T_j=\tilde{T}_{ir}\}=\dfrac{p_i}{n}$。

下面证明 $M_1,M_2,\cdots$ 和 $C_1,C_2,\cdots$ 是相互独立的。

首先，证明密文单元序列 $C_1,C_2,\cdots$ 是一列离散无记忆均匀分布或独立同均匀分布的随机序列，即对任意整数 $w>0$ 和任意 $c_1,c_2,\cdots,c_w\in C$，$C_1,C_2,\cdots$ 的 w 维离散分布满足

$$P\{C_1=c_1,C_2=c_2,\cdots,C_w=c_w\}=\frac{1}{n^w}=P\{C_1=c_1\}P\{C_2=c_2\}\cdots P\{C_w=c_w\} \tag{8}$$

利用概率论的知识，由已知条件可得

$$\begin{aligned}&P\{C_1=c_1,C_2=c_2,\cdots,C_w=c_w\}\\&=\sum_{m_1=0}^{n-1}\cdots\sum_{m_w=0}^{n-1}P\{C_1=c_1,C_2=c_2,\ldots,\\&C_w=c_w,M_1=m_1,M_2=m_2,\cdots,M_w=m_w\}\\&=\sum_{m_1=0}^{n-1}\cdots\sum_{m_w=0}^{n-1}P\{M_1=m_1,\cdots,M_w=m_w\}\\&P\{C_1=c_1,\cdots,C_w=c_w\,|\,M_1=m_1,\cdots,M_w=m_w\}\end{aligned} \tag{9}$$

其中，当 $\{M_1=m_1,\cdots,M_w=m_w\}$ 为不可能事件时，设式(9)中对应的乘积项为 0。由已知条件，对任一 (m_j,c_j)，在 $\tilde{K}_1,\tilde{K}_2,\cdots,\tilde{K}_q$ 中分别有唯一的实际密钥 $\tilde{k}_{1s_1}^{(j)}\in\tilde{K}_1,\tilde{k}_{2s_2}^{(j)}\in\tilde{K}_2,\cdots,\tilde{k}_{qs_q}^{(j)}\in\tilde{K}_q$，使 $c_j=E(\tilde{k}_{is_i}^{(j)},m_j)$，对任一 $j=1,2,\cdots,w$，$i=1,2,\cdots,q$ 和 $s_i\in\{1,2,\cdots,n\}$。因此

$$\begin{aligned}&P\{C_1=c_1,\cdots,C_w=c_w\,|\,M_1=m_1,\cdots,M_w=m_w\}\\&=P\left\{\sum_{i=1}^{q}\{K_1=\tilde{k}_{is_i}^{(1)}\},\cdots,\sum_{i=1}^{q}\{K_w=\tilde{k}_{is_i}^{(w)}\}\,\middle|\,M_1=m_1,\cdots,M_w=m_w\right\}\\&=\left[\sum_{i_1=1}^{q}P\{K_1=\tilde{k}_{i_1s_{i_1}}^{(1)}\}\right]\cdots\left[\sum_{i_w=1}^{q}P\{K_w=\tilde{k}_{i_ws_{i_w}}^{(w)}\}\right]\\&=\left[\sum_{i_1=1}^{q}\frac{p_{i_1}}{n}\right]\cdots\left[\sum_{i_w=1}^{q}\frac{p_{i_w}}{n}\right]=\frac{1}{n^w}\end{aligned} \tag{10}$$

进而

$$P\{C_1=c_1,C_2=c_2,\cdots,C_w=c_w\}=\frac{1}{n^w}\sum_{m_1=0}^{n-1}\cdots\sum_{m_w=0}^{n-1}P\{M_1=m_1,\cdots,M_w=m_w\}=\frac{1}{n^w}$$

于是，由 w 的任意性可得，$C_1,C_2,\cdots$ 是一列离散无记忆均匀分布的随机序列，即式(8)成立。

其次，由式(8)及其证明可得，对任意整数 $w>0$ 和 $m_1,m_2,\cdots,m_w\in M$ 与 $c_1,c_2,\cdots,c_w\in C$，有

$$\begin{aligned}&P\{M_1=m_1,M_2=m_2,\cdots,M_w=m_w,\\&\quad C_1=c_1,C_2=c_2,\cdots,C_w=c_w\}\\&=P\{M_1=m_1,\cdots,M_w=m_w\}\cdot\\&\quad P\{C_1=c_1,\cdots,C_w=c_w\mid M_1=m_1,\cdots,M_w=m_w\}\\&=\frac{P\{M_1=m_1,\cdots,M_w=m_w\}}{n^w}\\&=P\{M_1=m_1,M_2=m_2,\cdots,M_w=m_w\}\cdot\\&\quad P\{C_1=c_1,C_2=c_2,\cdots,C_w=c_w\}\end{aligned}\tag{11}$$

因此，对任意整数 $w>0$，随机向量 $(M_1,M_2,\cdots,M_w)$ 与 $(C_1,C_2,\cdots,C_w)$ 相互独立，因而这两个无限随机序列 $M_1,M_2,\cdots$ 和 $C_1,C_2,\cdots$ 也相互独立。由定义 4 可知，该保密通信系统是完善的。

证毕。

4.3 较现有完善保密性结论的优势

现有文献大都只是从实际应用角度出发讨论了有限保密通信的完善性，甚至可以说直接受到文献[1]的影响，文献[7-14]基本上只讨论某个基本密码系统的完善性，具有一定的片面性。与这些现有结果相比，本文所得结果有以下几个优点。

1) 本文研究了无限保密通信系统的完善性，给出了更严格的无限保密系统完善性的新概念，并获得了一类无限保密通信系统具有无限完善性的充分条件，该条件也可保证任一有限保密通信系统具有有限完善性。由此说明了本文所研究的无限保密通信系统的完善性是有意义和创新性的。

2) 本文定理 1 明确给出了密钥不等概率（即 $p_1,p_2,\cdots,p_q$ 不全相等）使用时具有完善保密性的一类保密通信系统具体可行的设计方法。

3) 本文所获结果在不要求明文具体统计特性的情况下，得到了密文序列是独立均匀分布的一种充分条件，这在更多考虑密码系统的安全性时需要进一步引入对明文均匀化处理提供了可能性。

5 二元加法完善流密码系统及其推广

考虑到现在公认常用的有限完善保密通信系统是基于“模加法运算”或“仿射变换”所设计的随机“一次一密”保密系统，下面将主要分析最常用的模 2 加法流密码完善系统的几个相关问题。

参照文献[2,4-6]，可以发现模 2 加法（有限或无限）流密码系统的基本明文空间、密文空间和实际密钥空间都为 $M=K=C=Z_2=\{0,1\}$。将加密变换的模 2 加法运算记为 $\oplus$，则其逆运算或模 2 减法运算 $\oplus^{-1}$ 仍然为模 2 加法运算 $\oplus$。因此，模 2 加法基本流密码系统的实际模型可表示为

$$\begin{aligned}\boldsymbol{\Phi}&=(M,K,C,\oplus,\oplus^{-1})=(M,K,C,\oplus,\oplus)\\&=(M=K=C=Z_2,\oplus)\end{aligned}\tag{12}$$

这样，现广泛使用的“二元加法流密码”实际上是反复利用该基本实际模型 $\boldsymbol{\Phi}$ 来进行保密通信的。

基本实际模型 $\boldsymbol{\Phi}$ 所确定的基本理论模型为 $\tilde{\boldsymbol{\Phi}}=(M,T=\{\tilde{T}_0,\tilde{T}_1\},C)$，其中，与实际密钥 $K=0$ 相互唯一对应的可逆变换 $\tilde{T}_0:M\leftrightarrow C$ 是恒等变换，且与 $K=1$ 相互唯一对应的可逆变换 $\tilde{T}_1:M\leftrightarrow C$ 是取反变换。$M=Z_2$ 上所有不同可逆变换只有 $\tilde{T}_0$ 和 $\tilde{T}_1$。

参照现有文献和本文结论，对模 2 加法随机“一次一密”无限完善保密通信系统介绍如下。

定理 2 在利用上述基本密码系统 $(M=C=Z_2,T=\{\tilde{T}_0,\tilde{T}_1\})$ 或 $(M=K=C=Z_2,\oplus)$ 进行所有可能的无限保密通信过程中，设密钥单元序列 $K_1,K_2,\cdots$ 或 $T_1,T_2,\cdots$ 是离散无记忆均匀分布随机序列，且与明文单元序列 $M_1,M_2,\cdots$ 相互独立，则该保密通信具有完善性。

显然，定理 2 是定理 1 的特殊情形。考虑到随机密钥单元序列在实际应用中会引起密钥管理上的极大困难，只能将定理 2 作为各种实用二元序列密码算法的理想模拟原型，具体方法通常是利用性能优良的伪随机密钥序列来替代离散无记忆均匀分布随机序列。

由上面的介绍可知，从保密通信意义上讲，上述二元加法基本流密码系统 $\boldsymbol{\Phi}$ 的设计可以说是唯一的。也就是说，长度为 1 bit 的二元基本密码系统 $\boldsymbol{\Phi}$ 的理论模型是唯一的，但其实际模型可以有很多种相互等价的不同形式。不过，超过 1 bit 的多元基本密码系统的理论模型设计并不唯一。

下面将先简单讨论把 1 bit 基本密码系统 $\boldsymbol{\Phi}$ 推广为多 bit 基本密码系统的理论模型的设计问题。

设 $n\geqslant 1$ 是一个整数，$Z_{2^n}=\{0,1,\cdots,2^n-1\}=\{0\cdots00,0\cdots01,\cdots,1\cdots11\}=Z_2^n$，则在 Z_{2^n} 上可定义两种常见的模 2^n 加法运算 $\oplus$ 和乘法运算 $\otimes$。可以验证，$(Z_{2^n},\oplus,\otimes)$ 是一个环。在该环中可定义线性函数，即对任意一对 $a,b\in Z_{2^n}$，将函数 $y=g(x)=a\otimes x\oplus b=ax\oplus b$ 称为环 $(Z_{2^n},\oplus,\otimes)$ 上的一个线性函数或仿射变换，对任意 $x\in Z_{2^n}$。下面将非仿射变

换也称为非线性函数。

在 Z_{2^n} 上还可定义逐比特异或运算 $\overline{\oplus}$：对任意 n bit $x=x_1x_2\cdots x_n, y=y_1y_2\cdots y_n\in Z_{2^n}$，和 $x_i,y_i\in Z_2$，$x\overline{\oplus}y=x_1x_2\cdots x_n\overline{\oplus}y_1y_2\cdots y_n=(x_1\oplus y_1)(x_2\oplus y_2)\cdots(x_n\oplus y_n)\in Z_2^n$。

这样，对任一 n bit $c\in Z_{2^n}$，可定义一个函数 $y=h(x)=x\overline{\oplus}c$，称之为逐比特异或函数或运算。为了区别，当将 Z_{2^n} 上的每个十进制整数看成是一个 n 比特数或向量时，将 Z_{2^n} 表示为 Z_2^n。

不难验证，当 $n=1$ 时，有 $\overline{\oplus}=\oplus$。此时，$(Z_2,\overline{\oplus})=(Z_2,\oplus)$，因而逐比特异或函数就是一个仿射函数。当 $n=2$ 时，可证 $(Z_2^2,\overline{\oplus})$ 上所有的 4 个逐比特异或函数都是环 $(Z_4,\oplus,\otimes)$ 上的线性函数。

将二元加法基本密码系统 $\boldsymbol{\Phi}$ 的明文集 Z_2 和密文集 Z_2 都推广为 $Z_{2^n}=Z_2^n$，对任意 $n=1,2,\cdots$。一般来说，当 n 较大时，在 $Z_{2^n}=Z_2^n$ 中如何设计基本理论密钥集 T 或实际密钥集 K 及其相关的加解密函数 E 与 D 是一个复杂的问题。因此，为了简化问题，下面以 $n=2$ 为例来讨论这种推广的基本密码系统的设计问题，可以大致看出多元基本密码系统设计的复杂性、多样性和灵活性。

在 $M=C=Z_{2^2}=\{0,1,2,3\}=\{00,01,10,11\}=Z_2^2$ 中，不同可逆变换总共有 $4!=24$ 个。这说明无论利用（无限多种中的）何种运算或变换来设计基本密码系统，所能利用的不同可逆加解密变换的数目最多为 24 个。如果所设计的密钥数量等于明文数量，则基本理论模型总共有 C_{24}^4 种不同的设计方法。因此，由保密系统第一种定义，理论上所能设计的不同基本理论密码系统的总数目为 $C_{24}^4=10\,626$。不过，其中会有一些可逆变换组不太适合同时用于设计基本密码系统。即使如此，可用于设计理论密钥的可逆变换组也是非常多的。下面举例说明几种特殊情形。

首先，考虑在 $M=C=Z_{2^2}=Z_2^2$ 中由反复利用逐比特异或运算所设计的基本密码系统 (M,C,T) 或 $(M,C,T=\{K,E\})=(M,C,K,E=D)$。此时，$K=\{00,01,10,11\}=Z_2^2=Z_4$ 和

$$\begin{aligned}y=y_1y_2&=x\overline{\oplus}k_1=x_1x_2\overline{\oplus}k_{11}k_{12}\\&=x_1x_2\overline{\oplus}00=x_1x_2=x=\tilde{T}_1(x)\end{aligned}$$

$$\begin{aligned}y=y_1y_2&=x\overline{\oplus}k_2=x_1x_2\overline{\oplus}k_{21}k_{22}=x_1x_2\overline{\oplus}01\\&=x_1\overline{x}_2=3x+1\bmod 4=3\otimes x\oplus 1=\tilde{T}_2(x)\end{aligned}$$

$$\begin{aligned}y=y_1y_2&=x\overline{\oplus}k_3=x_1x_2\overline{\oplus}k_{31}k_{32}\\&=x_1x_2\overline{\oplus}10=\overline{x}_1x_2=x+2\bmod 4=\tilde{T}_3(x)\end{aligned}$$

$$\begin{aligned}y=y_1y_2&=x\overline{\oplus}k_4=x_1x_2\overline{\oplus}k_{41}k_{42}\\&=x_1x_2\overline{\oplus}11=\overline{x}_1\overline{x}_2=3x+3\bmod 4=\tilde{T}_4(x)\end{aligned}$$

其中，$\overline{0}=1$ 和 $\overline{1}=0$，$x,y\in Z_4$，$K=\{k_1=00,k_2=01,k_3=10,k_4=11\}$，$T=\{\tilde{T}_1,\tilde{T}_2,\tilde{T}_3,\tilde{T}_4\}$，$\tilde{T}_j:Z_4\leftrightarrow Z_4$ 是一个可逆变换，$x_i,y_i,k_{ji}\in Z_2$ 和 $k_j=k_{j1}k_{j2}$，对任意 $i=1,2$ 和 $j=1,2,3,4$。这说明 Z_{2^2} 上所有的逐比特异或运算都是环 $(Z_{2^2},\oplus,\otimes)$ 上的线性运算。

其次，在环 $(Z_{2^2},\oplus,\otimes)$ 上的线性可逆变换总共有 8 个，因而环 $(Z_{2^2},\oplus,\otimes)$ 上的非线性可逆变换总共有 16 个，从中能找到 4 个非线性可逆变换组成一个拉丁方，如

$$\boldsymbol{L}=\begin{bmatrix}3&1&0&2\\0&2&1&3\\1&3&2&0\\2&0&3&1\end{bmatrix}\quad\boldsymbol{A}=\begin{bmatrix}1&0&2&3\\0&1&3&2\\3&2&0&1\\2&3&1&0\end{bmatrix}$$

$$\boldsymbol{B}=\begin{bmatrix}0&3&1&2\\1&2&0&3\\3&0&2&1\\2&1&3&0\end{bmatrix}\quad\boldsymbol{C}=\begin{bmatrix}3&1&0&2\\2&0&1&3\\0&2&3&1\\1&3&2&0\end{bmatrix}\tag{13}$$

甚至从这 16 个非线性可逆变换中也可以找到 12 个非线性可逆变换组成 3 个两两正交拉丁方组，如式(13)中的 $\{\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\}$ 就是一个两两正交拉丁方组。这样，利用一些非线性可逆变换组成的正交拉丁方组所设计的基本密码系统与现有二元加法流密码系统是完全不同的。在环 $(Z_{2^2},\oplus,\otimes)$ 上设计基本密码系统的方法要远比在环 $(Z_{2^2},\oplus,\otimes)$ 上只是重复利用单一基本密码系统 $\boldsymbol{\Phi}$ 所能设计出的一个基本密码系统 $(Z_{2^2},\overline{\oplus})$ 的方法要复杂得多。这也说明仅仅利用一个基本密码系统的多重形式来设计更多比特基本密码系统的方法是有局限性的，因而在现有模拟模 2 加法随机“一次一密”完善保密通信系统中所采用的多重形式基本密码系统的设计方法存在不足。

下面以具体例子来说明空间为 $Z_{2^2}=Z_2^2$ 的实际基本密码系统中加解密变换的一种设计方法。

将式(13)中的拉丁方 $\boldsymbol{L}$ 选为基本理论密码系统 $(M=C=Z_2^2, T=\boldsymbol{L})$，将与之相对应的某种实际基本密码系统 $(M=K=C=Z_2^2, E, D)$ 的实际加解密变换 E 和 D 按如下方法（可能不是唯一方法）进行设计：对任意 $m=m_1m_2, k=k_1k_2, c=c_1c_2 \in Z_{2^2}=Z_2^2$，

1)实际加密变换 E 为 $c=E(k,m)=m_2m_1+k+3 \bmod 4=\overleftarrow{m_1m_2}+k+3 \bmod 4$；

2) 实际解密变换 D 为 $m=D(k,c)=\overleftarrow{c-k-3 \bmod 4}$，其中，变换 $O(a)=\overleftrightarrow{a}=\overleftarrow{xy}=yx=b \in Z_4$ 表示将任意十进制数 $a \in Z_{2^2}$ 表示为 2 bit $a=xy \in Z_2^2$ 之后，再进行位置互换得到 2 bit 数值 $yx=b$，对任意 $a,b \in \{0,1,2,3\}$ 和 $x,y \in \{0,1\}$。

按照上述方法所设计的实际基本密码系统 $(M=K=C=Z_2^2, E, D)$，需要利用其进行实际保密通信时，结合具体保密通信条件，一种常用设计思路通常是以所能获得的完善保密通信系统作为理想目标去模拟设计出尽量接近完善保密性的伪随机“一次一密”保密通信系统。这完全可以仿照或借鉴现有常用的“模加法流密码”保密通信系统的设计方法，其基本思想是利用良好的伪随机密钥流序列来代替随机密钥流序列。其中的一个理论关键点是如何分析或评价伪随机序列的类随机性能“好坏”问题，另一个实际关键点是如何利用一些实用的规则来产生伪随机性能优良的密钥流序列问题。本文不再考虑相关问题。

6 结束语

本文将现有有限保密通信的完善保密性和“一次一密”保密系统推广为无限保密通信情形，研究了将正交拉丁方组应用于基本密码系统和无限完善保密通信系统之中的设计问题，并严格证明了所设计的随机“一次一密”无限保密通信系统具有完善保密性的一种充分条件，也可保证任一有限保密通信的完善保密性。这一理论结果为序列密码系统的设计提供了丰富且不同于现有常用的理想模拟原型，这对序列密码算法的相关理论研究具有较为明显的指导意义。

Shannon 曾指出，有限完善保密系统在实际应用中占有一席之地，它可能在安全性要求高和明文数量较少的场合中具有重要应用[1]。由此推测，本文所研究的无限完善保密系统在相关的场合中也具有一定的实际应用意义。从保密通信的安全性和实用性角度来看，本文所提出的多比特基本密码系统设计方法可以为序列密码算法提供一种全新且可行的设计方法，进而有可能进一步丰富序列密码设计理论。

参考文献：

[1] SHANNON C E. Communication theory of secrecy system[J]. Bell System Technical Journal, 1949, 28（4）：656-715.

[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 Z Z. The foundation of modern cryptography[M]. Beijing: Beijing University of Posts and Telecommunications, 2004.

[3] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Trans. On Info Theory, 1976, IT-22(6)：644-654.

[4] 胡向东, 魏琴芳. 应用密码学[M]. 北京: 电子工业出版社, 2006.
HU X D, WEI Q F. Applied cryptography[M]. Beijing: Electronic Industry Press, 2006.

[5] 温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数[M]. 北京: 科学出版社，2000.
WEN Q Y, NIU X X, YANG Y X. Boolean functions in modern cryptography[M]. Beijing: Science Press, 2000.

[6] 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 C S, XIAO G Z. Stream cryptography and its application[M]. Beijing: National Defense Industry Press, 1994.

[7] 魏仕民, 陈恺, 肖国镇, 等. 关于密码体制的完善保密性[J]. 通信学报, 2001, 22(7): 44-47.
WEI S M, CHEN K, XIAO G Z, et al. On perfect secrecy of cryptosystem[J]. Journal on Communications, 2001, 22(7): 44-47.

[8] 亢保元. 关于密码体制的完善保密性[J]. 中南大学学报, 2004, 35(3): 453-456.
KANG B Y. On perfect secrecy of cryptosystem[J]. Journal of Central South University, 2004, 35(3): 453-456.

[9] 王云光. 关于密码体制的完善保密性[J]. 大连理工大学学报, 2003, 43(S1): 69-71.
WANG Y G. Study of perfect secrecy of cryptosystem[J]. Journal of Dalian University of Technology, 2003, 43(S1): 69-71.

[10] STINSON D R. Cryptography theory and practice[M]. New York: CRC Press, 2005.

[11] 王勇, 朱芳来. 完善保密的再认识[J]. 计算机工程, 2007, 33(19): 155-157.
WANG Y, ZHU F L. Reconsideration of perfect secrecy[J]. Computer Engineering, 2007, 33(19): 155-157.

[12] 雷风宇, 崔国华, 徐鹏, 等. 完善保密体制的条件和存在性证明[J]. 计算机科学, 2010, 37(5): 99-102.
LEI F Y, CUI G H, XU P, et al. On the condition and the proof of the existence of perfect secrecy cryptosystem[J]. Computer Science, 2010, 37(5): 99-102.

[13] 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, 22(7): 44-47.
KANG B Y, WANG Y M. On the condition and design of perfect secrecy cryptosystem[J]. Journal on Communications, 2004, 25(2): 44-47.

[14] JUHA P. Symmetric blind decryption with perfect secrecy[J]. Journal of Computer Networks and Communications, 2017.

[15] 欧阳录. 幻方与幻立方的当代理论[M]. 湖南：湖南教育出版社，2004.
OUYANG L. The contemporary theory of magic cube and phantom cube[M]. Hunan: Hunan Education Press, 2004.

[16] 吴正声, 孙志人. 组合数学初步[M]. 南京: 南京师范大学出版社, 2001.
WU Z S, SUN Z R. Preliminary combinatorial mathematics[M]. Nanjing: Nanjing Normal University Press, 2001.

[17] 张里千. 关于正交拉丁方的最大数目(I)[J]. 数学进展, 1963, 6(2): 201-204.
ZHANG L Q. On the maximum number of orthogonal Latin squares (I)[J]. Advances in Mathematics, 1963, 6(2): 201-204.

[18] 李超. 用线性取余变换造正交拉丁方和幻方[J]. 应用数学学报, 1996, 19(2): 231-238.
LI C. Constructing orthogonal Latin squares and magic square by using linear congruent transformation[J]. Acta Mathematicae Applicatae Sinica, 1996, 19(2): 231-238.

[19] 陶照民. 偶阶幻方和奇阶正交拉丁方的构造方法[J]. 应用数学学报, 1983, 6(3): 276-281.
TAO Z M. The general methods for constructing even order magic squares and odd order orthogonal Latin squares[J]. Acta Mathematicae Applicatae Sinica, 1983, 6(3): 276-281.

[20] 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，2015，32（1）：32-39.
TIAN C J. Frequency irrelevance and its applications in one-key crypto systems[J]. Journal of Shenzhen University Science and Engineering. 2015, 32(1): 32-39.

[作者简介]

田传俊（1964−），男，湖北荆州人，博士，深圳大学教授，主要研究方向为伪随机性理论及其在信息安全中的应用。