基于分组可裂设计的分裂认证码的构造

王秀丽* 晋 霓 江雨杭
(中国民航大学理学院 天津 300300)

摘 要：分裂认证码是研究带仲裁的认证码的一种重要手段，相对无分裂认证码而言，分裂认证码大大提高了编码规则的利用率，该文主要通过可分组设计构造分裂认证码。首先给出了通过可分组设计(GDD)构造分裂认证码的定理，利用可分组设计构造可裂可分组设计，再由可裂可分组设计构造可裂平衡不完全区组设计(BIBD)，进而得到分裂认证码；验证在该文给定的条件下，通过可分组设计构造分裂认证码的可行性，在此基础上设计了一种可裂设计，构造了一组分裂认证码。计算所构造的分裂认证码的信源个数、编码规则个数、消息个数和假冒攻击成功概率及替代攻击成功概率等参数，并证明所构造的分裂认证码为最优分裂认证码。给出所构造的分裂认证码的具体例子，计算其假冒攻击成功概率、替代攻击成功概率，通过模拟仿真验证构造的合理性，并验证其满足最优性。

关键词：可分组设计；分裂认证码；可裂设计；平衡不完全区组设计；剩余类加群
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2022)02-0591-11
DOI: 10.11999/JEIT210683

Constructions of Splitting Authentication Codes Based on Group Divisible Design

WANG Xiuli JIN Ni JIANG Yuhang
(*College of Science*, *Civil Aviation University of China*, *Tianjin* 300300, *China*)

Abstract: Splitting authentication codes are an important method to study authentication codes with arbitration. Splitting authentication codes have a higher utilization rate of encoding rules than non-splitting authentication codes. Splitting authentication codes are constructed through group divisible design in this article. Firstly, a theorem for constructing splitting authentication codes is given. The theorem uses Group Divisible Design (GDD) to construct a splitting-GDD, and then a splitting-Balanced Incomplete Block Design (BIBD) by splitting-GDD is constructed, and then a splitting authentication code is obtained; Secondly, the feasibility of constructing splitting authentication codes through GDD under the conditions given in this article is verified. Then a splitting design is given and a splitting authentication codes based on GDD is constructed; Thirdly, the number of sources, the number of encoding rules, the number of messages of the splitting authentication code, the impersonation attack probability and the substitution attack probability are calculated, then this article proves that the constructed splitting authentication code is an optimal splitting authentication code; Finally, a concrete example of the constructed splitting authentication code is given, the successful impersonation attack probability and the successful substitution attack probability are calculated, the rationality of construction is verified by simulation, and verifies that it satisfies the optimality.

Key words: Group Divisible Design(GDD); Splitting authentication codes; Splitting design; Balanced Incomplete Block Design(BIBD); Residue class additive group

收稿日期：2021-07-08；改回日期：2021-10-29；网络出版：2021-11-06
*通信作者： 王秀丽 xlwangcauc@163.com
基金项目：中央高校基本科研业务费中国民航大学自然科学类重点项目(3122019192)
Foundation Item: The Key Projects of Natural Science from Fundamental Research of the Central Universities of China Civil Aviation University (3122019192)

1 引言

信息安全的主要内容包括信息的保密以及信息的认证。保密和认证是两件不同的事情。信息的认证，指的是信息的接收方能够认证判断收到的信息是否完整或者是否来自真正的发送方，当接收方收到一个信息时，能够确认这条信息是来自真正发送方的真实信息，而不是由敌人假冒发送方发送的虚假信息，或者能确认这条信息在传输过程当中没有被敌人替换修改。构造认证码是确保信息的可认证性，降低未发现欺骗的可能性的一个重要方法。

认证码的认证功能大致可以分为保证发送方的真实性，保障信息传输的完整性，确保发送方和接收方相互不可抵赖，以及对访问权限的是否合法进行判断，共4大类。发送方的真实性指的是真正的发送方发出的信息确实被接收方所接收。信息传输的完整性指的是，存储的信息或者在传输过程中的信息没有因各种因素被篡改、丢失等。发送方和接收方的不可抵赖性指的是，发送方和接收方不得对已发送或接收的信息进行否认。访问权限的合法性指的是，当授权用户申请访问信息时，确保该用户能够顺利访问已获授权的各种数据资源，相对应的是，当其他非授权用户申请访问信息时，保证其无法访问到受保护的信息。在很多的认证过程中，通常包括发送方、接收方以及敌人，发送方给接收方发送信息，敌人想要冒充发送方给接收方发送虚假的信息，或者对发送方发给接收方的信息进行截获、篡改，改变发送方向接收方传达的信息以达到欺骗接收方的目的，此时发送方和接收方是相互信任的。在三方认证模型中，当发送方和接收方可能相互欺骗时，就需要在认证模型中增添仲裁方。

分裂认证码是研究带仲裁的认证码的一种重要手段。分裂认证码相对无分裂认证码而言，大大提高了编码规则的利用率，能够达到信源个数多且编码规则个数少的目的。

认证码的概念最早由Gilbert等人[1]提出，1985年Simmons[2]首次提出了一种更普遍和系统的认证理论。

分裂认证码的概念由王永传等人[3]在1999年提出，并通过分裂认证码，进一步得到纠错码。提出了认证码的最大假冒攻击成功概率与最大替代攻击成功概率相等时，信源数目与编码规则数目呈现线性正相关。

Ogata等人[4]在2004年，给出了外部差分族(External Difference Families, EDF)、外部平衡不完全区组设计 (External Balanced Incomplete Block Designs, EBIBD)、分裂平衡不完全区组设计(Splitting Balanced Incomplete Block Designs, Splitting BIBD)3种组合设计，并通过分裂不完全区组设计，给出了一种最优分裂认证码。

2005年，Ge等人[5]从组合设计的角度研究了最佳的c-分裂认证码。给出了用于最优c-分裂认证码的各种组合构造，存在具有u个信源和v个消息的最优c-分裂认证码的必要条件为：$(u,c)=(2,2t)$；$(u,c)=(2,3)\,v\neq 10$；$(u,c)=(3,2)\,v\neq 9$；$(u,c)=(4,2)\,v\neq 49,385$。

2008年，刘金龙等人[6]提出了基于循环排列的迭代法以及基于正交排列的迭代法构造Cartesian认证码的两种方法。这两种方法有效地减少了编码规则的数目。

2009年，裴定一[7]给出了欺骗成功概率的信息论下界，得到了密钥个数的下界，并证明了当编码规则数目取到下界的时候，欺骗攻击成功概率等于信息论下界。同时也给出了使密钥个数等于下界的完善认证系统的组合特征。

Wang等人[8]在2010年证明了$(v,3\times 3,\lambda)$-分裂平衡不完全区组设计存在的必要条件：$v\geq uc$，$\lambda(v-1)\equiv 0\,(\mathrm{mod}c\,(u-1))$以及$\lambda v\,(v-1)\equiv 0\ \left(\mathrm{mod}c^2\right.$ $\left.u\,(u-1)\right)$ 在满足$(v,\lambda)\notin\{(55,1),(39,9k):k=1,2,\cdots\},\lambda\neq 0\,(\mathrm{mod}54),v\neq 0\,(\mathrm{mod}2)$ 的条件下也是充分的。

Liang等人[9]于2017年提出了最优的带约束的强部分平衡t设计(Optimal Restricted Strong Partially Balanced block Design, ORSPBD)可用于构造满足组合下界或信息论下界的分裂认证码。他们证明了在满足任意的正整数$v\equiv v_0\mathrm{mod}\left(2c^2\right)$，$v_0\in\left\{1\leq x\leq 2c^2:\gcd(x,c)=1\text{ or }\gcd(x,c)=\right\}/\{c^2+1\leq x\leq(c+1)^2:\gcd(x,c)=1\text{ and }\gcd(x,2)=2\}$的条件下，ORSPBD$(v,2\times c,1)$都存在。

2018年，Li等人[10]定义了一种新的设计，并称为正交多重阵列。此外，Li等人[10]证明了该设计的存在意味着存在最优的c-分裂认证码。

2 预备知识

本节介绍区组设计、平衡不完全区组设计、可分组设计的相关概念、定义、定理；介绍分裂认证码的相关概念，欺骗攻击成功概率的计算方式以及满足最优分裂认证码的条件。为之后通过可分组设计构造分裂认证码提供理论基础。

2.1 区组设计的基本概念

组合设计[11]，是一种将集合里的元素划分成为满足某些特定性质子集的布局方法。组合设计的主要类别为：平衡不完全区组设计，正交阵列和拉丁方，成对平衡设计以及Hadamard和正交设计。本

文主要利用组合设计中的区组设计构造可分裂认证码。

下面给出区组设计的定义。

定义1 [12] 令V为一个有限集合，且$|V|=v$，V中的元素称为样品；$\boldsymbol{B}$为V的包含k个元素的子集的集合，且$|\boldsymbol{B}|=b$，这些子集$B_1,B_2,\cdots,B_b$称为区组。由所有$k-$子集构成的簇$\boldsymbol{B}=\{B_1,B_2,\cdots,B_b\}$称为样品集合$V$上的一个区组设计，其中$k,v$为正整数且$2\le k\le v$，本文称$(V,\boldsymbol{B})$是$V$的一个平衡区组设计，如果$V$的任意$t$元素恰好同时出现在$\lambda$个区组里，其中正整数$\lambda$称为设计指数。(针对$2\le k\le v$的条件，如果$k=1$，那么区组内不含元素对且$l=0$。)

当$k<v$, $t=2$时，称为平衡不完全区组设计(简称BIBD)。

定义2 [12] 设v,k,λ为3个给定的正整数，$D=(V,\boldsymbol{B})$为一个序偶，若满足以下条件：

(1) $|V|=v$；

(2) 对于任意的$B\in\boldsymbol{B}$，都有$k_B=k$；

(3) 对于任意的$p,q\in V,p\ne q$，都有$\lambda_{p,q}=\lambda$。

本文就称D是一个平衡不完全区组设计，简称区组设计或BIBD，记作$B(k,\lambda,v)$。v称为D的阶，k称为D的区组容量或区组长度，λ称为相遇数或指数。

下面给出BIBD存在的必要条件：

定理1 [12] 假设$B(k,\lambda,v)$存在，那么：

(1) $\lambda(v-1)\equiv 0\,(\mathrm{mod}(k-1))$；

(2) $\lambda v(v-1)\equiv 0\,(\mathrm{mod}k(k-1))$。

2.2 可裂平衡不完全区组设计(Splitting BIBD)

首先给出t-可裂设计的概念。

定义3 [13] 令t,v,b,c,u,λ为正整数，序偶$(V,\boldsymbol{B})$是一个$t-(v,c\times u;\lambda)$可裂设计，其中$c\times u\le u$且$t\le u$，且该序偶满足：

(1) V为一个包含v个元素的集合；

(2)$\boldsymbol{B}$为V中包含k个元素的区组的集合，且对于任意的区组$B_i\in\boldsymbol{B}$ $(1\le i\le b)$都可以表示成u个不相交的集合的并集，即$B_i=B_{i1}\cup B_{i2}\cup\cdots\cup B_{iu}$，其中$|B_{ij}|=c(1\le j\le u)$；

(3)V中的每一个$t-$子集$\{x_m\}_{m=1}^{t}$都恰好包含在λ个区组$B_i=B_{i1}\cup B_{i2}\cup\cdots\cup B_{iu}$当中，使得$x_m\in B_{ij_m}(1\le j_m\le u)$，对于任意的$1\le m\le t$，且$j_1,j_2,\cdots,j_m$互不相等。

当$t=2$时，得到下面可裂不完全区组设计(Splitting BIBD)的定义。

定义4 [8] 设v,b,λ为3个给定的正整数，$D=(V,\boldsymbol{B})$为一个序偶，若满足以下条件：

(1)$|V|=v$，$|\boldsymbol{B}|=b$；

(2)对于任意的区组$B_i\in\boldsymbol{B}$，可以表示为u个互不相交子集的并集，即$B_i=B_{i1}\cup B_{i2}\cup B_{i3}\cup\cdots\cup B_{iu}$，其中$|B_{i1}|=|B_{i2}|=\cdots=|B_{iu}|=c$，且对任意的$B_i\in\boldsymbol{B}$都有$B_i|=k=c\times u$；

(3)对于任意的$p,q\in V,p\ne q$都恰好包含在λ个区组B_i中使得$p\in B_{ij},q\in B_{in}$且$j\ne n$；

则称D是一个$(v,c\times u,\lambda)-$可裂BIBD。

下面给出Splitting BIBD存在的必要条件：

定理2 [8] 假设$B(k,\lambda,v)$存在，那么：

(1) $\lambda(v-1)\equiv 0\ (\mathrm{mod}(u-1)c)$；

(2) $\lambda v(v-1)\equiv 0\ (\mathrm{mod}u(u-1)c^2)$。

定理3 [8] 假设$(V,\boldsymbol{B})$是一个$(v,c\times u,\lambda)-$splitting BIBD，V中的元素x_i包含在r个区组当中，b为$\boldsymbol{B}$中区组的个数，那么以下两个等式成立

$$r=\lambda(v-1)/(u-1)c \tag{1}$$

$$b=\lambda v(v-1)/u(u-1)c^2 \tag{2}$$

例1 令$(V,\boldsymbol{B})$是一个$(9,2\times 2,1)-$Splitting BIBD，其中$V=Z_9$，$\boldsymbol{B}$为$B_1=\{(0,1),(2,4)\}$, $B_2=\{(1,2),(3,5)\}$, $B_3=\{(2,3),(4,6)\}$, $B_4=\{(3,4),(5,7)\}$, $B_5=\{(4,5),(6,8)\}$, $B_6=\{(5,6),(7,0)\}$, $B_7=\{(6,7),(8,1)\}$, $B_8=\{(7,8),(0,2)\}$, $B_9=\{(8,0),(1,3)\}$的并集，V中的每一个元素都恰好包含在4个区组当中。

定理4[5] 假设$(V,\boldsymbol{B})$是一个$(v,3\times 2,1)-$Splitting BIBD，其存在的充要条件是$v\equiv 1,9\,(\mathrm{mod}24)$，但$v\ne 9$。

2.3 可分组设计相关知识

2.3.1 可分组设计(GDD)

定义5 [12] 设u,λ为两个给定的正整数，K,M为两个给定正整数集，设$D=(V,\boldsymbol{G},\boldsymbol{B})$为一个3元组，其中$V$为一个$v$元集，$\boldsymbol{G}$构成$V$的一个划分，$\boldsymbol{G}$的元素称为组(group)，$\boldsymbol{B}$的元素称为区组。若下述条件满足：

(1) 对于任意的$B\in\boldsymbol{B}$，都有$|B|\in K$；

(2) 对于任意的$G\in\boldsymbol{G}$，都有$|G|\in M$；

(3) 对于任意的$B\in\boldsymbol{B}$与任意的$G\in\boldsymbol{G}$，都有$|G\cap B|\le 1$；

(4) V中任意一对属于不同组的元素恰好同时包括在λ个区组中。

则称D为一个可分组设计(Group Divisible Design, GDD)，记作$GD(K,\lambda,M;v)$。

当$K=\{k\},M=\{m\}$时，就称$GD(K,B,M;v)$为均匀可分组设计，且$GD(\{k\},B,\{m\};v)$可简记为$GD(k,\lambda,m;v)$。

定义6[12] 设$D=(V,\boldsymbol{G},\boldsymbol{B})$是一个$GD(K,\lambda,M;v)$，如果对$1\le i\le s$，$\boldsymbol{G}$中包含$t_i$个大小为$m_i$的组，并且满足$v=\sum_{i=1}^{s}t_im_i$，那么称$GD(K,\lambda,M;v)$的型为$m_1^{t_1}m_2^{t_2}\cdots m_s^{t_s}$。

下面给出均匀GDD存在的必要条件：

定理5[12] 假设$GD(k,\lambda,m;v)$存在，那么：

(1) $\lambda(v-m)\equiv 0\,(\mathrm{mod}(k-1))$;

(2) $\lambda v(v-m)\equiv 0\,(\mathrm{mod}k(k-1))$;

(3) $v\equiv 0\,(\mathrm{mod}m)$, $v=m$或$v\ge km$。

定理6[9] 假设$(V,\boldsymbol{G},\boldsymbol{B})$是一个$GD(k,\lambda,m;v)$，$V$中的元素$x_i$包含在$r$个区组当中，$b$为$\boldsymbol{B}$中区组的个数，那么有式(3)和式(4)两个等式成立

$$r=\lambda(v-m)/(k-1) \tag{3}$$

$$b=\lambda v(v-m)/k(k-1) \tag{4}$$

定理7[12] $GD(3,\lambda,m;v)$存在的必要条件$\lambda(v-m)\equiv 0\,(\mathrm{mod}(k-1))$，$\lambda v(v-m)\equiv 0\,(\mathrm{mod}k(k-1))$, $v\equiv 0\,(\mathrm{mod}m)$, $v=m$或$v\ge km$也是充分的。

2.3.2 可裂可分组设计(Splitting GDD)

下面给出Splitting GDD的定义：

定义7[5] 设u,c,λ为3个给定的正整数，K,M为两个给定正整数集，设$D=(V,\boldsymbol{G},\boldsymbol{B})$为一个3元组，其中$V$为一个$v$元集，$\boldsymbol{G}$构成$V$的一个划分，$\boldsymbol{G}$的元素称为组(group)，$\boldsymbol{B}$的元素称为区组。若下述条件满足：

(1)对于任意的$B_i\in\boldsymbol{B}$，B_i可以表示为u个大小为$c\in K$的互不相交的子集；

(2)$B_i=B_{i1}\cup B_{i2}\cup B_{i3}\cup\cdots\cup B_{iu}$；

(3)对于任意的$G\in\boldsymbol{G}$，都有$|G|\in M$；

(4)对于任意的$B\in\boldsymbol{B}$与任意的$G\in\boldsymbol{G}$，都有$|G\cap B|\le 1$；

(5)V中任意一对属于不同组的元素p，q都恰好同时包括在λ个区组中，并且满足$p\in B_{ij},q\in B_{in}$且$j\ne n$；

则称D为一个可裂可分组设计或Splitting GDD。

定理8[5] 设$D=(V,\boldsymbol{G},\boldsymbol{B})$是一个GDD，令$w$：$V\to N\cup\{0\}$为一个权函数，并且对于任意的$x,y\in V$都有$w(x)=w(y)$，对于每一个区组$B\in\boldsymbol{B}$，假如存在一个型为$(w(x)\,|x\in B)$的$u\times c-$splitting GDD，$\left(\bigcup_{x\in B}S(x),\{S(x)\,|x\in B\},A(\boldsymbol{B})\right)$，其中$S(x)=\{(x,1),(x,2),(x,3),\cdots,(x,w(x))\,|\,x\in V\}$，那么就存在这样一个型为$\left(\sum_{x\in G}w(x)\,|G\in\mathcal{G}\right)$的$u\times c-$splitting GDD，$\left(\bigcup_{x\in G}S(x),\left\{\bigcup_{x\in G}S(x)\,|\,G\in\mathcal{G}\right\},\bigcup_{B\in\boldsymbol{B}}A(\boldsymbol{B})\right)$。

定理9[5] 令u,c为两个正整数，且$u\ge 2,c\ge 2$，令$D=(V,\boldsymbol{G},\boldsymbol{B})$是一个$\{u\}-$GDD，$w:V\to N\cup\{0\}$为一个权函数，且对于任意的$x\in V$都有$w(x)=c$，那么存在一个型为$\left(\sum_{x\in G}w(x)\,|G\in\mathcal{G}\right)$的$u\times c-$splitting GDD。

2.3.3 Splitting GDD与Splitting BIBD之间的关系

可裂可分组设计与可裂平衡不完全区组设计在一定条件下可以相互转化，下面给出Splitting GDD转换成Splitting BIBD的条件：

定理10[8] 令$D=(V,\boldsymbol{G},\boldsymbol{B})$是一个$(u\times c,1)-$splitting GDD，假如对于任意的$G\in\boldsymbol{G}$，$(G\cup\{\infty\},\boldsymbol{B}_G)$都是一个$(|G|+1,,u\times c,1)-$splitting BIBD，那么$(V\cup\{\infty\},\boldsymbol{B}^*)$为一个$(|V|+1,u\times c,1)-$splitting BIBD，且$\boldsymbol{B}^*=\boldsymbol{B}\cup\left(\bigcup_{G\in\boldsymbol{G}}\boldsymbol{B}_G\right)$。

关于可分组设计的最新成果，可参见文献[13–17]。

2.4 认证码的相关概念

2.4.1 分裂认证码的概念

令S表示信源的有限集合，M表示消息的有限集合，E表示编码规则的有限集合。发送方在发送消息之前，通过安全信道将编码规则传送给接收方，之后使用编码规则$e\in E$加密信源$s\in S$，以获得消息$m=e(s)$通过信道发送。如果在同一编码规则$e\in E$下使用不止一个消息来传达特定的信源$s\in S$，则认为该认证码具有分裂性[18]。分裂认证码的例子见表1。

在这个定义中，一条消息$m\in M$计算为$m=e(s,r)$，其中r表示从某些指定的有限集R中选择的随机数。定义[5]

$$e(s):=\{m\in M:m=e(s,r)\,r\in R\} \tag{5}$$

对于任意编码规则$e\in E$和任意信源$s\in S$，分裂意味着对于一些$e\in E$和一些$s\in S$，满足$|e(s)|>1$。为了确保接收方能够解密正在发送的消息，当$s\ne s'$时，对于任意的$e\in E$满足$e(s)\cap e(s')=\phi$。

对于给定的编码规则$e\in E$，设

$$M(e):=\bigcup_{s\in S}e(s) \tag{6}$$

表示对e有效的消息集。对于编码规则e和不同消息的集合$M'\subseteq M(e)$，定义[13]

$$f_e(M'):=\{s\in S:e(s)\cap M'\ne\phi\} \tag{7}$$

即一组信源将根据编码规则e由M'中的消息进行编码。当且仅当$m\in M(e)$时，接收到的消息m将被接收方接收为真实消息。当满足此条件时，接收方通过应用解码规则e^{-1}解密消息m，其中$e^{-1}(m)=s,m=e(s,r),r\in R$。

表 1　分裂认证码的示例

	s_1	s_2
e_1	$\{m_1, m_2\}$	$\{m_3, m_5\}$
e_2	$\{m_2, m_3\}$	$\{m_4, m_6\}$
e_3	$\{m_3, m_4\}$	$\{m_5, m_7\}$
e_4	$\{m_4, m_5\}$	$\{m_6, m_8\}$
e_5	$\{m_5, m_6\}$	$\{m_7, m_9\}$
e_6	$\{m_6, m_7\}$	$\{m_8, m_1\}$
e_7	$\{m_7, m_8\}$	$\{m_9, m_2\}$
e_8	$\{m_8, m_9\}$	$\{m_1, m_3\}$
e_9	$\{m_9, m_1\}$	$\{m_2, m_4\}$

如果(S, M, E)对于任意编码规则$e \in E$和任意信源$s \in S$满足以下条件，$|e(s)| = c$，则称其为c-分裂认证码。

对于每个编码规则$e \in E$和每个信源$s \in S$。我们注意到，认证码可以用一个$(|E| \times |S|)$-编码矩阵表示，其中的行由编码规则$e \in E$标记，信源$s \in S$标记列，并且元素由$a_{se} = e(s)$定义[18]。

2.4.2　欺骗攻击成功概率

首先介绍两种攻击方式。

假冒攻击[5]是指，在发送消息前，发送方和接收方约定所使用的密钥e，这时敌方可以将M中任意消息$m \in M$发送给接收方，本文称这种攻击方式为假冒攻击。如果接收方以密钥e接收了该消息，那么称敌人假冒攻击成功，反之，如果接收方拒绝了该消息，则称敌人假冒攻击失败。用P_0表示假冒攻击成功的概率

$$P_0 = \frac{\max\limits_{m \in M} |\{e \in E | e(s) = m\}|}{|E|} \tag{8}$$

接下来介绍替代攻击[5]。

当发送方向接收方发送了一条消息m，敌方截获这条消息之后，选取了另外的一个信源s'，通过密钥e得到消息m'，并替代m，将m'发送给了接收方，本文将这种攻击方式称为替代攻击。当$m' \in e(s')$，且$m \in e(s)$时，称敌人替代攻击成功，反之则失败。用P_1表示替代攻击成功的概率

$$P_1 = \frac{\max\limits_{m \neq m'} |\{e \in E | e(s) = m, e(s') = m'\}|}{\{e \in E | e(s) = m\}} \tag{9}$$

2.4.3　分裂认证码满足最优的条件

对于c-分裂认证码(S, M, E)，首先给出欺骗攻击成功概率的下界以及编码规则的数目：

引理1[5]　在分裂认证码(S, M, E)中，其假冒攻击概率

$$P_0 \geq \frac{|\{e \in E | e(s) = m\}|}{|E|} \tag{10}$$

引理2[5]　在分裂认证码(S, M, E)中，其替代攻击概率：

$$P_1 \geq \frac{|\{e \in E | e(s) = m, e(s') = m'\}|}{|\{e \in E | e(s) = m\}|} \tag{11}$$

引理3[5]　由引理1、引理2可得

$$|E| \geq \frac{|\{e \in E | e(s) = m, e(s') = m'\}|}{P_0 P_1} \geq \frac{1}{P_0 P_1} \tag{12}$$

即在分裂认证码(S, M, E)中，有$P_0 P_1 \geq 1/|E|$。

引理4[4]　如果一个分裂认证码(S, M, E)的欺骗攻击成功概率能取到其信息论下界，那么称该分裂认证码(S, M, E)为最优分裂认证码。

3　基于可分组设计构造分裂认证码

3.1　分裂认证码的构造定理

首先给出由可裂BIBD构造分裂认证码的引理。

给定一个$(v, u \times c, 1) - $splitting BIBD$(X, \boldsymbol{B})$，令消息集$M = X$，信源集$S = \{s_1, \cdots, s_i, \cdots, s_u\}$，对于每个区组$B \in \boldsymbol{B}$，把它定义为一个编码规则$e \in E$且$e(s_1) = B_1, \cdots, e(s_i) = B_i, \cdots, e(s_u) = B_u$，其中$B_i (1 \leq i \leq u)$是区组$B$的第$i$行元素的集合，它是一个$1 \times c$的行向量，意味着把信源$s_i$加密成$c$个消息，于是得到下面的引理。

引理5[8]　如果存在一个$(v, u \times c, 1) - $splitting BIBD，那么就存在一个c-分裂认证码，其中：

(1) $|M| = v, |S| = u$；

(2) 每一个信源出现的概率都相等。

由引理4以及引理5，可以得到由可裂BIBD构造最优分裂认证码的定理：

引理6[8]　如果存在一个$(v, u \times c, 1) - $splitting BIBD，那么就存在一个最优分裂认证码，使得

(1)$|M| = v, |S| = u$；

(2)每一个信源出现的概率都相等；

(3)$P_0 = \dfrac{\max\limits_{m \in M} |\{e \in E | e(s) = m\}|}{|E|}$；

$P_1 = \dfrac{\max\limits_{m \neq m'} |\{e \in E | e(s) = m, e(s') = m'\}|}{\{e \in E | e(s) = m\}}$；其中编码规则定义为$e_i(s_j) = B_{ij} (1 \leq i \leq v,\ 1 \leq j \leq u)$。

接下来给出由均匀GDD构造2-分裂认证码的定理。

定理11　设t为一个正整数，$t \geq 3$且$8t + 1 \equiv 1, 9 \pmod{24}$，$D = (V, \boldsymbol{G}, \boldsymbol{B})$是一个$GD(3, 1, 4t; v)$，其中$v = 12t$，那么存在一个$(24t + 1, 3 \times 2, 1) - $splitting BIBD。

证明　$GD(3, 1, 4t; 12t)$可通过定理8中权函

数w，扩展得到一个$3\times 2-$splitting GDD。由定理10可得，若要证明存在一个$(2\times|V|+1,3\times 2,1)-$splitting BIBD，只需要证明$3\times 2-$splitting GDD中任意的$G\in\boldsymbol{G}$，$(G\cup\{\infty\},\boldsymbol{B}_G)$都是一个$(|G|+1,,3\times 2,1)-$splitting BIBD，由定理4可知：$|G|+1=8t+1\equiv 1,9\,(\mathrm{mod}24)$，所以$(2\times|V|+1,3\times 2,1)-$splitting BIBD一定存在，并且$\boldsymbol{B}^{*}=\boldsymbol{B}\cup\left(\bigcup_{G\in\boldsymbol{G}}\boldsymbol{B}_G\right)$。

由引理5，就存在一个2-分裂认证码，其中$|M|=24t+1,|S|=3$；每一个信源出现的概率都相等。 证毕

3.2 基于可分组设计构造分裂认证码

3.2.1 基于可分组设计构造2–分裂认证码

假设V是一个模$12t$的剩余类加群，将其记为Z_{12t}，所以V中的元素可以表示为

$$V=\{0,1,\cdots,12t-1\} \tag{13}$$

根据定义4，将V划分成为3个大小为$4t$的组，即$\boldsymbol{G}=G_1\cup G_2\cup G_3$，将这3个组表示出来

$$G_1=\{0,1,2,\cdots,4t-1\} \tag{14}$$

$$G_2=\{4t,4t+1,\cdots,8t-1\} \tag{15}$$

$$G_3=\{8t,8t+1,\cdots,12t-1\} \tag{16}$$

可以得到一个型为$(4t)^3$的均匀$GD(3,1,4t;v)$。令

$$B_1=(0,4t,8t) \tag{17}$$

$$B_2=(0,4t+1,8t+1) \tag{18}$$

$$\vdots$$

$$B_{4t}=(0,8t-1,12t-1) \tag{19}$$

$$B_{4t+1}=(1,4t,8t+1) \tag{20}$$

$$\vdots$$

$$B_{8t}=(1,8t-1,8t) \tag{21}$$

$$B_{8t+1}=(2,4t,8t+2) \tag{22}$$

$$\vdots$$

$$B_{12t}=(2,8t-1,8t+1) \tag{23}$$

$$\vdots$$

$$B_{4t(4t-1)+1}=(4t-1,\ 4t,\ 12t-1) \tag{24}$$

$$B_{4t(4t-1)+2}=(4t-1,\ 4t+1,\ 8t) \tag{25}$$

$$\vdots$$

$$B_{16t^2}=(4t-1,8t-1,12t-1+4t-1) \tag{26}$$

对于任意的$B_i=(x_1,x_2,x_3)\,(1\le i\le 16t^2)$，若存在$x_j\notin G_i(1\le j\le 3)$，那么令$x_i{}'=x_i-4t$，其中$x_i{}'\in G_i$，将变换后的$B_i$记为$B_i{}'$，则$\boldsymbol{B}=\bigcup_{i=1}^{16t^2}B_i'$。

现在证明$(V,\boldsymbol{G},\boldsymbol{B})$是一个$GD(3,1,4t;12t)$。

对于任意的$B\in\boldsymbol{B}$与任意的$G\in\boldsymbol{G}$，都有$|B|=3,|G|=4t,\ |G\cap B|=1$，且$V$中任意一对属于不同组的元素恰好同时包含在1个区组中，满足GDD的定义。且在$GD(3,1,4t;12t)$中，$k=3,\lambda=1,v=12t,m=4t$，进而有

$$(12t-4t)=8t\equiv 0\,(\mathrm{mod}(3-1)) \tag{27}$$

$$12t\,(12t-4t)=96t^2\equiv 0\,(\mathrm{mod}3(3-1)) \tag{28}$$

$$12t\equiv 0\,(\mathrm{mod}4t) \tag{29}$$

满足定理5，可知$(V,\boldsymbol{G},\boldsymbol{B})$是一个$GD(3,1,4t;12t)$。

下面将上述的$GD(3,1,4t;12t)$变为一个$3\times 2-$splitting GDD。

定义一个权函数

$$w:V\to V'=\bigcup_{i=1}^{12t}\{(x_i,0),(x_i,1)\,|x_i\in V\} \tag{30}$$

由定理8、定理9可得，令u,c为两个正整数，且$u=3,c=2$，那么存在一个$(V',\boldsymbol{G}',\boldsymbol{B}')$，它是一个型为$(8t)^3$的$3\times 2-$splitting GDD，其中$\boldsymbol{G}'$为

$$G_1'=\{(0,0),(0,1),(1,0),(1,1),\cdots,(4t-1,0),(4t-1,1)t\} \tag{31}$$

$$G_2'=\{(4t,0),(4t,1),(4t+1,0),(4t+1,1),\cdots,(8t-1,0),(8t-1,1)\} \tag{32}$$

$$G_3'=\{(8t,0),(8t,1),\cdots,(12t-1,0),(12t-1,1)\} \tag{33}$$

的并集。它的区组为

$$B_1'=\begin{pmatrix}(0,0)&(0,1)\\(4t,0)&(4t,1)\\(8t,0)&(8t,1)\end{pmatrix},$$

$$B_2'=\begin{pmatrix}(0,0)&(0,1)\\(4t+1,0)&(4t+1,1)\\(8t+1,0)&(8t+1,1)\end{pmatrix},\cdots,$$

$$B_{4t}'=\begin{pmatrix}(0,0)&(0,1)\\(8t-1,0)&(8t-1,1)\\(12t-1,0)&(12t-1,1)\end{pmatrix},$$

$$B_{4t+1}'=\begin{pmatrix}(1,0)&(1,1)\\(4t,0)&(4t,1)\\(8t+1,0)&(8t+1,1)\end{pmatrix},\cdots,$$

$$B_{8t}'=\begin{pmatrix}(1,0)&(1,1)\\(8t-1,0)&(8t-1,1)\\(8t,0)&(8t,1)\end{pmatrix},$$

$$B_{8t+1}'=\begin{pmatrix}(2,0)&(2,1)\\(4t,0)&(4t,1)\\(8t+2,0)&(8t+2,1)\end{pmatrix},\cdots,$$

$$B_{12t}'=\begin{pmatrix}(2,0)&(2,1)\\(8t-1,0)&(8t-1,1)\\(8t+1,0)&(8t+1,1)\end{pmatrix},$$

$$B'_{12t+1}=\begin{pmatrix}(3,0)&(3,1)\\(4t,0)&(4t,1)\\(8t+3,0)&(8t+3,1)\end{pmatrix},\cdots$$

$$B'_{16t}=\begin{pmatrix}(3,0)&(3,1)\\(8t-1,0)&(8t-1,1)\\(8t+2,0)&(8t+2,1)\end{pmatrix},\cdots$$

$$B'_{4t(4t-1)+1}=\begin{pmatrix}(4t-1,0)&(4t-1,1)\\(4t,0)&(4t,1)\\(12t-1,0)&(12t-1,1)\end{pmatrix},$$

$$B'_{4t(4t-1)+2}=\begin{pmatrix}(4t-1,0)&(4t-1,1)\\(4t+1,0)&(4t+1,1)\\(8t,0)&(8t,1)\end{pmatrix},\cdots,$$

$$B'_{16t^2}=\begin{pmatrix}(4t-1,0)&(4t-1,1)\\(8t-1,0)&(8t-1,1)\\(12t-2,0)&(12t-2,1)\end{pmatrix}。$$

令 $B'_i=B'_{i1}\cup B'_{i2}\cup B'_{i3}(1\le i\le 16t^2)$，$|B'_{i1}|=|B'_{i2}|=|B'_{i3}|=2$，对于任意的$G'\in\boldsymbol{G}',B\in\boldsymbol{B}$，都有$|G'|=8t$，且$|G'\cap B'|=1$，考虑$V$中任意一对属于不同组的元素$p,q$，都恰好包含在1个区组当中，且满足$p\in B'_{ij},q\in B'_{in}$且$j\ne n$。所以这是一个$(3\times 2,1)-$splitting GDD。

现在证明对于任意的$G'\in\boldsymbol{G}'$，存在$(G'\cup\{\infty\},\boldsymbol{B}_{G'})$是一个$(|G'|+1,3\times 2,1)-$splitting BIBD。

由定理4可得，对于任意的$G'\in\boldsymbol{G}',|G'|=8t$，当$t$满足$(8t+1)\equiv 1,9\ (\mathrm{mod}24)$时，都存在一个$(8t+1,3\times 2,1)-$splitting BIBD，所以存在$(G'\cup\{\infty\},B_b)$是一个$(|G'|+1,3\times 2,1)-$splittingBIBD。

由定理10可得，根据上述条件可知，存在一个$(|V'|+1,3\times 2,1)-$splitting BIBD，其区组为$\boldsymbol{B}^*=\boldsymbol{B}'\cup\left(\bigcup_{G'\in\boldsymbol{G}'}\boldsymbol{B}_{G'}\right)$。

结论　通过上述构造，可以得到一个$2-(24t+1,24t^2+t,3\times 2,1)-$splitting BIBD，进一步得到一个2–分裂认证码，它的参数为$|S|=3,|M|=24t+1$，其中t满足$(8t+1)\equiv 1,9\ (\mathrm{mod}24)$。

接下来计算该2-分裂认证码的欺骗攻击成功概率。

由上述可知，认证码编码规则的个数等于所构造的Splitting BIBD中区组的个数，即$|E|=b$，由定理3中式子(2)$|E|=b=\dfrac{\lambda v(v-1)}{u(u-1)c^2}=\dfrac{1(24t+1)24t}{3(3-1)2^2}=24t^2+t$。

已知每一个信源S出现的概率都相等，编码规则e在Z_{24t+1}中呈现均匀分布，因此，假冒攻击成功概率为：$P_0=\dfrac{\max\limits_{m\in M}|\{e\in E|\,e(s)=m\}|}{|E|}=\dfrac{(24t+1-1)/2(3-1)}{24t^2+t}=\dfrac{6}{24t+1}$，引理1中式(10)等号成立。

替代攻击成功概率为

$$P_1=\frac{\max\limits_{m\ne m'}|\{e\in E|\,e(s)=m,e(s')=m'\}|}{\{e\in E|\,e(s)=m\}}=\frac{1}{(24t+1-1)/2(3-1)}=\frac{1}{6t}$$

引理2中式(11)等号成立。

由上述计算结果可得$P_0P_1=\dfrac{6}{24t+1}\times\dfrac{1}{6t}=\dfrac{1}{24t^2+t}=\dfrac{1}{|E|}$，故满足引理4的条件，所以该2-分裂认证码为最优分裂认证码。

3.2.2 基于2-可裂设计$(Z_{73},\boldsymbol{B})$的2-分裂认证码

当$t=3$时，假设V是一个模36的剩余类加群，那么V中的元素可以表示为$V=\{0,1,2,3,\cdots,34,35\}$，按照3.2.1节中方法构造一个$GD(3,1,12;36)$，其中组为$G_1=\{0,1,2,3,4,5,6,7,8,9,10,11\}$，$G_2=\{12,13,14,15,16,17,18,19,20,21,22,23\}$，$G_3=\{24,25,26,27,28,29,30,31,32,33,34,35\}$，区组为$B_1=(0,12,24),B_2=(0,13,25),\cdots,B_{12}=(0,23,35),B_{13}=(1,12,25),B_{14}=(1,13,26),\cdots,B_{24}=(1,23,24)$，$B_{25}=(2,12,26),B_{26}=(2,13,27),\cdots,B_{36}=(2,23,25),B_{37}=(3,12,27),B_{38}=(3,13,28),\cdots,B_{48}=(3,23,26),\cdots$，$B_{133}=(11,12,35),B_{134}=(11,13,24),\cdots,B_{144}=(1,23,34)$。

由上述构造，通过3.2.1节中定义的权函数w，能够得到一个$3\times 2-$splitting GDD相应的组为$G_1=\{(0,0),(0,1),(1,0),(1,1),\cdots(11,0),(11,1)\}$；$G_2=\{(12,0),(12,1),(13,0),(13,1),\cdots(23,0),(23,1)\}$; $G_3=\{(24,0),(24,1),(25,0),(25,1),\cdots(35,0),(35,1)\}$；相应的区组为

$$B'_1=\begin{pmatrix}(0,0)&(0,1)\\(12,0)&(12,1)\\(24,0)&(24,1)\end{pmatrix},B'_2=\begin{pmatrix}(0,0)&(0,1)\\(13,0)&(13,1)\\(25,0)&(25,1)\end{pmatrix},\cdots,$$

$$B'_{12}=\begin{pmatrix}(0,0)&(0,1)\\(23,0)&(23,1)\\(35,0)&(35,1)\end{pmatrix},B'_{13}=\begin{pmatrix}(1,0)&(1,1)\\(12,0)&(12,1)\\(25,0)&(25,1)\end{pmatrix},$$

$$B'_{14}=\begin{pmatrix}(1,0)&(1,1)\\(13,0)&(13,1)\\(26,0)&(26,1)\end{pmatrix},\cdots,B'_{24}=\begin{pmatrix}(1,0)&(1,1)\\(23,0)&(23,1)\\(24,0)&(24,1)\end{pmatrix},$$

$$B'_{25}=\begin{pmatrix}(2,0)&(2,1)\\(12,0)&(12,1)\\(26,0)&(261)\end{pmatrix},B'_{26}=\begin{pmatrix}(2,0)&(2,1)\\(13,0)&(13,1)\\(27,0)&(27,1)\end{pmatrix},\cdots,$$

$$B'_{36}=\begin{pmatrix}(2,0)&(2,1)\\(23,0)&(23,1)\\(25,0)&(25,1)\end{pmatrix},B'_{37}=\begin{pmatrix}(3,0)&(3,1)\\(12,0)&(12,1)\\(27,0)&(27,1)\end{pmatrix},$$

$$B'_{38}=\begin{pmatrix}(3,0)&(3,1)\\(13,0)&(13,1)\\(28,0)&(28,1)\end{pmatrix},\cdots,B'_{48}=\begin{pmatrix}(3,0)&(3,1)\\(25,0)&(25,1)\\(26,0)&(26,1)\end{pmatrix},\cdots,$$

$B'_{133}=\begin{pmatrix}(11,0)&(11,1)\\(12,0)&(12,1)\\(35,0)&(35,1)\end{pmatrix}$, $B'_{134}=\begin{pmatrix}(11,0)&(11,1)\\(13,0)&(13,1)\\(24,0)&(24,1)\end{pmatrix}$, $\cdots$, $B'_{144}=\begin{pmatrix}(11,0)&(11,1)\\(23,0)&(23,1)\\(34,0)&(34,1)\end{pmatrix}$。对于每个$G_1,G_2,G_3\in\boldsymbol{G}$，将其元素对应标为序号1, 2, $\cdots$, 24，添加一个点∞对应标号为0，运算时按照标号进行运算，则得到3组25个样本集。定义3个$(24+1,3\times2,1)-$splitting BIBD的基区组分别

$$\boldsymbol{B}_{G_1}=\begin{pmatrix}(0,0)&(0,1)\\(1,0)&(2,0)\\(6,0)&(10,0)\end{pmatrix},\boldsymbol{B}_{G_2}=\begin{pmatrix}(12,0)&(12,1)\\(13,0)&(14,0)\\(18,0)&(22,0)\end{pmatrix},$$

$$\boldsymbol{B}_{G_3}=\begin{pmatrix}(24,0)&(24,1)\\(25,0)&(26,0)\\(30,0)&(34,0)\end{pmatrix}$$。记$\boldsymbol{B}_{G_1}$, $\boldsymbol{B}_{G_2}$, $\boldsymbol{B}_{G_3}$分别为上面这3个Splitting BIBD的基区组中元素下标+1(mod25)后得到的区组的集合。可得$(V\cup\{\infty\},\boldsymbol{B}^*)$是一个$(73,3\times2,1)-$splitting BIBD。其中$\boldsymbol{B}^*=B'_1\cup B'_2\cup\cdots\cup B'_{144}\cup\boldsymbol{B}_{G_1}\cup\boldsymbol{B}_{G_2}\cup\boldsymbol{B}_{G_3}$可以得到如表2的2-分裂认证码$(3,73,219)$。

由表2可以看出：$|S|=3,|M|=73,|e(s)|=2$，计算得到$|E|=219$，假冒攻击成功的概率为$P_0=18/219=6/73$，由此可知等于引理1中假冒攻击成功概率的下界；替代攻击成功的概率为$P_1=1/18$，同样满足引理2中替代攻击成功概率的下界；同时有$P_0P_1=1/|E|=1/219$。故满足引理4，所以该2-分裂认证码$(3,73,219)$为最优分裂认证码。

为了验证构造的合理性，对编码矩阵进行数值仿真，结果如图1所示。

仿真分析 图1是以消息集M为横坐标，编码规则集E为纵坐标。可以看出对于每个消息，都对应有18个有效的编码规则，故假冒攻击成功概率为

$$P_0=\frac{\max\limits_{m\in M}|\{e\in E|\,e(s)=m\}|}{|E|}=\frac{18}{219}=\frac{6}{73}\tag{34}$$

进一步对替代攻击成功概率进行模拟仿真。

仿真分析 图2的横坐标和纵坐标分别用消息集M标记，竖坐标用编码规则集E标记。可以看出对于横坐标和纵坐标所代表的任意两个不同的消息同时有效的编码规则个数为1，故替代攻击成功的概率为

$$P_1=\frac{\max\limits_{m\neq m'}|\{e\in E|\,e(s)=m,e(s')=m'\}|}{\{e\in E|\,e(s)=m\}}=\frac{1}{18}\tag{35}$$

综上分析可知：仿真结果与构造结果一致，故本文的构造是合理的。

3.2.3 基于2-可裂设计(Z_{97},B)的2-分裂认证码

当$t=4$时，$24t+1=97$，令V是一个模48的剩余类加群，V中的元素可以表示为$V=\{0,1,2,3,\cdots,46,47\}$。

按照3.2.1节中方法构造一个$GD(3,1,16;48)$，其中组$G_1=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$，$G_2=\{16,17,18,19,20,21,22,23,24,25,26,27,$

表 2 2-分裂认证码$(3,73,219)$

	s_1	s_2	s_3
e_1	$\{m_1,m_2\}$	$\{m_{25},m_{26}\}$	$\{m_{49},m_{50}\}$
e_2	$\{m_1,m_2\}$	$\{m_{27},m_{28}\}$	$\{m_{51},m_{52}\}$
e_3	$\{m_1,m_2\}$	$\{m_{29},m_{30}\}$	$\{m_{53},m_{54}\}$
e_4	$\{m_1,m_2\}$	$\{m_{31},m_{30}\}$	$\{m_{55},m_{56}\}$
e_5	$\{m_1,m_2\}$	$\{m_{33},m_{30}\}$	$\{m_{57},m_{58}\}$
e_6	$\{m_1,m_2\}$	$\{m_{35},m_{30}\}$	$\{m_{59},m_{60}\}$
e_7	$\{m_1,m_2\}$	$\{m_{37},m_{30}\}$	$\{m_{61},m_{62}\}$
e_8	$\{m_1,m_2\}$	$\{m_{39},m_{30}\}$	$\{m_{63},m_{64}\}$
e_9	$\{m_1,m_2\}$	$\{m_{41},m_{30}\}$	$\{m_{65},m_{66}\}$
e_{10}	$\{m_1,m_2\}$	$\{m_{43},m_{30}\}$	$\{m_{67},m_{68}\}$
e_{11}	$\{m_1,m_2\}$	$\{m_{45},m_{30}\}$	$\{m_{69},m_{70}\}$
e_{12}	$\{m_1,m_2\}$	$\{m_{47},m_{30}\}$	$\{m_{71},m_{72}\}$
e_{13}	$\{m_1,m_2\}$	$\{m_3,m_5\}$	$\{m_{13},m_{21}\}$
e_{14}	$\{m_6,m_7\}$	$\{m_8,m_{10}\}$	$\{m_{18},m_1\}$
e_{15}	$\{m_{14},m_{15}\}$	$\{m_{16},m_{18}\}$	$\{m_1,m_9\}$
e_{16}	$\{m_{22},m_{23}\}$	$\{m_{24},m_1\}$	$\{m_9,m_{17}\}$
e_{17}	$\{m_{24},m_{73}\}$	$\{m_1,m_3\}$	$\{m_{11},m_{19}\}$
e_{18}	$\{m_{73},m_1\}$	$\{m_2,m_4\}$	$\{m_{12},m_{20}\}$
...	...	...	...

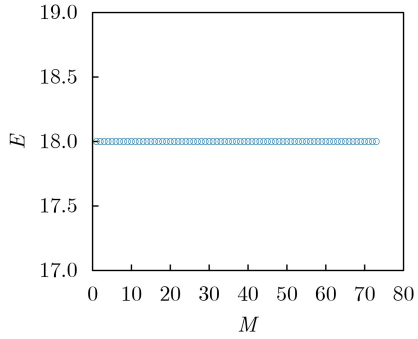

图 1 分裂认证码$(3,73,219)$模仿攻击成功概率模拟仿真

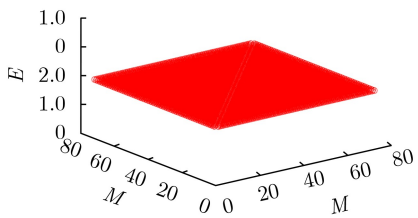

图 2 分裂认证码$(3,73,219)$替代攻击成功概率模拟仿真

$28,29,30,31\}$，$G_3=\{32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47\}$。区组$B_1=(0,16,32)$，$B_2=(0,17,33),\cdots,B_{16}=(0,31,47)$，$B_{17}=(1,16,33),B_{18}=(1,17,34),\cdots,B_{32}=(1,31,32)$，$B_{33}=(2,16,34),B_{34}=(2,17,35),\cdots,B_{48}=(2,31,33)$，$B_{49}=(3,16,35),B_{50}=(3,17,36),\cdots,B_{64}=(3,31,34),\cdots,B_{241}=(15,16,47),B_{242}=(15,17,32),\cdots,B_{256}=(15,31,46)$。

通过3.2.1节中定义的权函数w的构造，同样能得到一个$3\times 2-$splitting GDD，这个设计的组为

$$G_1=\{(0,0),(0,1),(1,0),(1,1),\cdots(15,0),(15,1)\}$$
$$G_2=\{(16,0),(16,1),(17,0),(17,1),\cdots(31,0),(31,1)\}$$
$$G_3=\{(32,0),(32,1),(33,0),(33,1),\cdots(47,0),(47,1)\}$$

区组为

$$B_1'=\begin{pmatrix}(0,0)&(0,1)\\(16,0)&(16,1)\\(32,0)&(32,1)\end{pmatrix},B_2'=\begin{pmatrix}(0,0)&(0,1)\\(17,0)&(17,1)\\(33,0)&(33,1)\end{pmatrix},\cdots,$$
$$B_{16}'=\begin{pmatrix}(0,0)&(0,1)\\(31,0)&(31,1)\\(47,0)&(47,1)\end{pmatrix},B_{17}'=\begin{pmatrix}(1,0)&(1,1)\\(16,0)&(16,1)\\(33,0)&(33,1)\end{pmatrix},$$
$$B_{18}'=\begin{pmatrix}(1,0)&(1,1)\\(17,0)&(17,1)\\(34,0)&(34,1)\end{pmatrix},\cdots,B_{32}'=\begin{pmatrix}(1,0)&(1,1)\\(31,0)&(31,1)\\(32,0)&(32,1)\end{pmatrix},$$
$$B_{33}'=\begin{pmatrix}(2,0)&(2,1)\\(16,0)&(16,1)\\(34,0)&(34,1)\end{pmatrix},B_{34}'=\begin{pmatrix}(2,0)&(2,1)\\(17,0)&(17,1)\\(35,0)&(35,1)\end{pmatrix},\cdots,$$
$$B_{48}'=\begin{pmatrix}(2,0)&(2,1)\\(31,0)&(31,1)\\(33,0)&(33,1)\end{pmatrix},B_{49}'=\begin{pmatrix}(3,0)&(3,1)\\(16,0)&(16,1)\\(35,0)&(35,1)\end{pmatrix},$$
$$B_{50}'=\begin{pmatrix}(3,0)&(3,1)\\(17,0)&(17,1)\\(36,0)&(36,1)\end{pmatrix},\cdots,B_{64}'=\begin{pmatrix}(3,0)&(3,1)\\(33,0)&(331)\\(34,0)&(34,1)\end{pmatrix},\cdots,$$
$$B_{241}'=\begin{pmatrix}(15,0)&(151)\\(16,0)&(16,1)\\(47,0)&(47,1)\end{pmatrix},B_{242}'=\begin{pmatrix}(15,0)&(15,1)\\(17,0)&(17,1)\\(32,0)&(32,1)\end{pmatrix},\cdots,$$
$$B_{256}'=\begin{pmatrix}(15,0)&(15,1)\\(31,0)&(31,1)\\(46,0)&(46,1)\end{pmatrix}。$$

对于任意的$G_i\in\boldsymbol{G}(1\le i\le 4)$，将其元素对应标为序号1, 2, ⋯, 32，添加一个点∞对应标号为0，运算时按照标号进行运算，则得到3组33个样本集。定义$(33,3\times 2,1)-$splitting BIBD的基区组为

$$\begin{pmatrix}x_3&x_5\\x_4&x_{18}\\x_{15}&x_{29}\end{pmatrix},\begin{pmatrix}x_1&x_{18}\\x_{10}&x_{20}\\x_{14}&x_{31}\end{pmatrix},$$
$$\begin{pmatrix}x_3&x_{29}\\x_{12}&x_{13}\\x_{19}&x_{31}\end{pmatrix},\begin{pmatrix}x_1&x_{11}\\x_3&x_{29}\\x_8&x_{30}\end{pmatrix}\tag{36}$$

$(33,3\times 2,1)-$splitting BIBD的区组为上述基区组下标+3 (mod33)，将区组的集合分别记作$\boldsymbol{B}_{G_1}$, $\boldsymbol{B}_{G_2}$, $\boldsymbol{B}_{G_3}$。

可得$(V\cup\{\infty\},\boldsymbol{B}^*)$是一个$(97,3\times 2,1)-$splitting BIBD，其中：$\boldsymbol{B}^*=B_1'\cup B_2'\cup\cdots\cup B_{256}'\cup\boldsymbol{B}_{G_1}\cup\boldsymbol{B}_{G_2}\cup\boldsymbol{B}_{G_3}$，进而得到一个2–分裂认证码$(3,97,388)$，如表3所示。

其中$|S|=3,|M|=97,|E|=388,|e(s)|=2$。假冒攻击成功的概率为$P_0=24/388=6/97$，引理1中式(10)等号成立；替代攻击成功的概率为$P_1=1/24$，引理2中式(11)等号成立；由上述计算结果可知，$P_0P_1=1/|E|=1/388$，所以引理3中等号也成立，进而引理4成立；则该2-分裂认证码$(3,97,388)$也是最优分裂认证码。

为了验证构造的合理性，对编码矩阵进行数值仿真，结果如图3所示。

仿真分析　图3是以消息集M为横坐标，以编码规则集E为纵坐标，可以看出对于每个消息，都对应有24个编码规则，故假冒攻击成功概率为$P_0=\dfrac{\max\limits_{m\in M}|\{e\in E|e(s)=m\}|}{|E|}=\dfrac{24}{388}=\dfrac{6}{97}$；下面进一步分析替代攻击成功概率，如图4所示。

仿真分析　在上述3维图像中，x轴、y轴都代表消息集，z轴为编码规则集。可以看出对x轴、y轴所代表的任意两个不同的消息同时有效的编码规则个数均为1，故替代攻击成功的概率为$P_1=\dfrac{\max\limits_{m\ne m'}|\{e\in E|e(s)=m,e(s')=m'\}|}{\{e\in E|e(s)=m\}}=\dfrac{1}{24}$。

综上分析可知：仿真结果与构造结果一致，本文的构造是合理的。

3.3　与相关构造的对比分析

本节将把本文构造方法与相应结果，与其他文章作对比，如表4所示。(为了方便表示，将其他论文按照参考文献中的论文标号进行表示。)

由表4可知：相对于已有构造方法，本文所提使用加权函数将GDD变为可裂GDD，通过可裂GDD进一步得到可裂BIBD，并最终获得最优2-分裂认证码的方法，更加简单直观。这种方法使得参数更加多变，为构造信源数目为3的分裂认证码提供了新思路。

4　结束语

消息认证是认证技术最主要的应用，是网络信息安全领域中非常值得关注和研究的问题。分裂认证码是消息认证的一个重要组成部分，它可用于身份认证、门限认证方案等，也是构造带仲裁的认证码的一种重要手段，大大提高了编码规则的利用率。

表 3 2–分裂认证码$(3,97,388)$

	s_1	s_2	s_3
e_1	$\{m_1,m_2\}$	$\{m_{33},m_{34}\}$	$\{m_{65},m_{66}\}$
e_2	$\{m_1,m_2\}$	$\{m_{35},m_{36}\}$	$\{m_{67},m_{68}\}$
e_3	$\{m_1,m_2\}$	$\{m_{37},m_{38}\}$	$\{m_{69},m_{70}\}$
e_4	$\{m_1,m_2\}$	$\{m_{39},m_{40}\}$	$\{m_{71},m_{72}\}$
e_5	$\{m_1,m_2\}$	$\{m_{41},m_{42}\}$	$\{m_{73},m_{74}\}$
e_6	$\{m_1,m_2\}$	$\{m_{43},m_{44}\}$	$\{m_{75},m_{76}\}$
e_7	$\{m_1,m_2\}$	$\{m_{45},m_{46}\}$	$\{m_{77},m_{78}\}$
e_8	$\{m_1,m_2\}$	$\{m_{47},m_{48}\}$	$\{m_{79},m_{80}\}$
e_9	$\{m_1,m_2\}$	$\{m_{49},m_{50}\}$	$\{m_{81},m_{82}\}$
e_{10}	$\{m_1,m_2\}$	$\{m_{51},m_{52}\}$	$\{m_{83},m_{84}\}$
e_{11}	$\{m_1,m_2\}$	$\{m_{53},m_{54}\}$	$\{m_{85},m_{86}\}$
e_{12}	$\{m_1,m_2\}$	$\{m_{55},m_{56}\}$	$\{m_{87},m_{88}\}$
e_{13}	$\{m_1,m_2\}$	$\{m_{57},m_{58}\}$	$\{m_{89},m_{90}\}$
e_{14}	$\{m_1,m_2\}$	$\{m_{59},m_{60}\}$	$\{m_{91},m_{92}\}$
e_{15}	$\{m_1,m_2\}$	$\{m_{61},m_{62}\}$	$\{m_{93},m_{94}\}$
e_{16}	$\{m_1,m_2\}$	$\{m_{63},m_{64}\}$	$\{m_{95},m_{96}\}$
e_{17}	$\{m_{97},m_2\}$	$\{m_1,m_{15}\}$	$\{m_{12},m_{26}\}$
e_{18}	$\{m_1,m_{18}\}$	$\{m_{10},m_{20}\}$	$\{m_{14},m_{31}\}$
e_{19}	$\{m_{25},m_9\}$	$\{m_1,m_{11}\}$	$\{m_5,m_{20}\}$
e_{20}	$\{m_5,m_{22}\}$	$\{m_{14},m_{24}\}$	$\{m_{18},m_1\}$
e_{21}	$\{m_{24},m_{17}\}$	$\{m_{97},m_1\}$	$\{m_7,m_{19}\}$
e_{22}	$\{m_{18},m_{11}\}$	$\{m_{27},m_{28}\}$	$\{m_1,m_{13}\}$
e_{23}	$\{m_6,m_{32}\}$	$\{m_{15},m_{18}\}$	$\{m_{22},m_1\}$
e_{24}	$\{m_1,m_{11}\}$	$\{m_3,m_{29}\}$	$\{m_8,m_{30}\}$
...	...	...	...

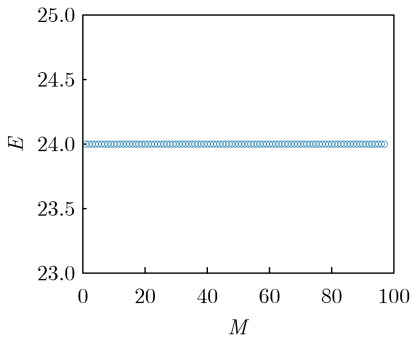

图 3 分裂认证码$(3,97,388)$模仿攻击成功概率模拟仿真

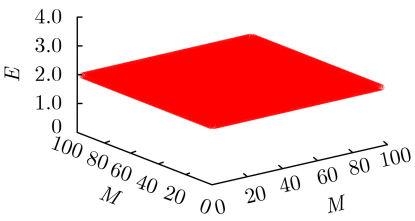

图 4 分裂认证码$(3,97,388)$替代攻击成功概率模拟仿真

表 4 本文与其他文献构造方法比较

文献[4]	通过EDF构造可裂BIBD得到最优分裂认证码，在该文献中给出的例子的信源数2，少于本文的信源数3。
文献[6]	文献[6]构造的分裂认证码不是最优的，本文所构造的分裂码是最优的。
文献[18]	该文献给出了可裂设计与分裂认证码的对应定理，但并没有给出具体的构造方法，只给出了部分简单的例子，并且信源数较少。本文对GDD加权后得到可裂GDD，通过可裂GDD得到可裂BIBD，构造方法巧妙，组合结构清楚，给出了信源数相对较多的分裂认证码的例子，并针对具体实例，对构造的合理性进行了仿真分析。

通过可裂设计构造分裂认证码，主要思想是把区组划分成一些不相交的子区组的并，其中子区组的大小就是分裂数，子区组的个数即为信源数。这种思想方法可用于多用户认证，即通信双方通常为多人甚至是群体的情况，也可用于与信息安全密切相关的密钥共享、无线传感器网络，密码认证，隐私保护用户模型工业4.0的前向保密认证方案[19–22]等，上述内容将在今后的研究中进行深入探索。

对于本文利用GDD构造可裂设计，进而构造分裂数大于2以及信源数大于3的情况，是需要今后继续研究的内容。

参 考 文 献

[1] GILBERT E N, MACWILLIAMS F J, and SLOANE N J A. Codes which detect deception[J]. *The Bell System Technical Journal*, 1974, 53(3): 405–424. doi: 10.1002/j.1538-7305.1974.tb02751.x.

[2] SIMMONS G J. Authentication Theory/Coding Theory[M]. BLAKLEY G R, CHAUM D. Advances in Cryptology: Proceedings of CRYPTO 84. Berlin Heidelberg: Springer-Verlag, 1985: 411–431.

[3] 王永传, 杨义先. 分裂认证码与纠错码[J]. 通信保密, 1999(1): 64–66.
WANG Yongchuan and YANG Yixian. Spliting authentication codes with and error-correcting codes[J]. *Information Security and Communications Privacy*, 1999(1): 64–66.

[4] OGATA W, KUROSAWA K, STINSON D R, *et al*. New combinatorial designs and their applications to authentication codes and secret sharing schemes[J]. *Discrete Mathematics*, 2004, 279(1/3): 383–405.

[5] GE Gennian, MIAO Ying, and WANG Lihua. Combinatorial constructions for optimal splitting authentication codes[J]. *Discrete Mathematics*, 2005, 18(4): 663–678.

[6] 刘金龙, 许宗泽. CARTESIAN认证码的原理及构造[J]. 电子与信息学报, 2008, 30(1): 93–95.
LIU Jinlong and XU Zongze. On the theory and construction of CARTESIAN authentication codes[J]. *Journal of Electronics & Information Technology*, 2008,

30(1): 93–95.

[7] 裴定一. 消息认证码[M]. 合肥: 中国科学技术大学出版社, 2009.
PEI Dingyi. Message Authentication Codes[M]. Hefei: China University of science and Technology Press, 2009.

[8] WANG Jinhua and SU Renwang. Further results on the existence of splitting BIBDs and application to authentication codes[J]. *Acta Applicandae Mathematicae*, 2010, 109(3): 791–803. doi: 10.1007/s10440-008-9346-8.

[9] LIANG Miao, JI Lijun, and ZHANG Jingcai. Some new classes of 2-fold optimal or perfect splitting authentication codes[J]. *Cryptography and Communications*, 2017, 9(3): 407–430. doi: 10.1007/s12095-015-0179-9.

[10] LI Mingchao, LIANG Miao, DU Beiliang, *et al*. A construction for optimal c-splitting authentication and secrecy codes[J]. *Designs, Codes and Cryptography*, 2018, 86(8): 1739–1755. doi: 10.1007/s10623-017-0421-x.

[11] COLBOURN C J and DINITZ J H. Handbook of Combinatorial Designs[M]. Boca Raton: CRC Press, 1996.

[12] 沈灏. 组合设计理论[M]. 上海: 上海交通大学出版社, 2008.
SHEN Hao. Theory of Combinatorial Designs[M]. Shanghai: Shanghai Jiao Tong University Press, 2008.

[13] SAURABH S and SINHA K. Some new resolvable group divisible designs[J/OL]. *Communications in Statistics-Theory and Methods*, 2020. doi: 10.1080/03610926.2020.1817487.

[14] FORBES A D. Group divisible designs with block size four and type $g^u b^1 (gu/2)^1$[J]. *Graphs and Combinatorics*, 2020, 36(6): 1687–1703. doi: 10.1007/s00373-020-02213-5.

[15] ABEL R J R, BUNJAMIN Y A, and COMBE D. Some new group divisible designs with block size 4 and two or three group sizes[J]. *Journal of Combinatorial Designs*, 2020, 28(8): 614–628. doi: 10.1002/jcd.21719.

[16] XU Hengzhou, YU Zhongyang, FENG Dan, *et al*. New construction of partial geometries based on group divisible designs and their associated LDPC codes[J]. *Physical Communication*, 2020, 39: 100970. doi: 10.1016/j.phycom.2019.100970.

[17] HUANG Yupei, LIU Chiaan, CHANG Y, *et al*. A family of group divisible designs with arbitrary block sizes[J]. *Taiwanese Journal of Mathematics*, 2019, 23(6): 1291–1302.

[18] HUBER M. Combinatorial bounds and characterizations of splitting authentication codes[J]. *Cryptography and Communications*, 2010, 2(2): 173–185. doi: 10.1007/s12095-010-0020-4.

[19] VISHNU V I and PUTHALI H B. Techniques for validating and sharing secrets[P]. USA, Patent, 20120159645, 2012.

[20] 王晨宇, 汪定, 王菲菲, 等. 面向多网关的无线传感器网络多因素认证协议[J]. 计算机学报, 2020, 43(4): 683–700. doi: 10.11897/SP.J.1016.2020.00683.
WANG Chenyu, WANG Ding, WANG Feifei, *et al*. Multi-factor user authentication scheme for multi-gateway wireless sensor networks[J]. *Chinese Journal of Computers*, 2020, 43(4): 683–700. doi: 10.11897/SP.J.1016.2020.00683.

[21] LI Zengpeng, WANG Ding, and MORAIS E. Quantum-safe round-optimal password authentication for mobile devices[J/OL]. *IEEE Transactions on Dependable and Secure Computing*, 2020. doi: 10.1109/TDSC.2020.3040776.

[22] WANG Chenyu, WANG Ding, XU Guoai, *et al*. Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0[J/OL]. Science China (Information Sciences). https://kns.cnki.net/kcms/detail/11.5847.TP.20210820.1521.008.html, 2021.

王秀丽：女，1976年生，副教授，硕士生导师，研究方向为代数、组合、密码及编码.

晋　霓：女，1998年生，硕士生，研究方向为代数、组合、密码及编码.

责任编辑：余　蓉