文章编号: 1008-1542(2011)01-0011-04

# 用射影几何构作新的 $A^2$-码

张晓寒[1], 王文贤[2]

(1. 衡水职业技术学院基础部, 河北衡水　053000; 2. 河北师范大学数学与信息科学学院, 河北石家庄　050016)

摘　要: 利用射影几何构作了一个新的带仲裁的认证码, 并计算了它的参数。进一步假设全部规则是按等概率分布选择的, 分别计算了 5 种攻击成功的概率。

关键词: 认证码; 带仲裁的认证码; 射影几何

中图分类号: O157.4　　文献标志码: A

# New construction of $A^2$-codes based on projective geometry

ZHANG Xiao-han[1], WANG Wen-xian[2]

(1. Department of Basic Courses, Hengshui Vocational Technology Institute, Hengshui Hebei 053000, China; 2. Mathematics and Information Science College, Hebei Normal University, Shijiazhuang Hebei 050016, China)

**Abstract:** In this paper, a new construction of $A^2$-codes based on projective geometry is given, and the parameters are computed. Assuming that the probability distribution of all the rules are uniform, the probabilities of successful attacks are also computed.

**Key words:** authentication codes; authentication codes with arbitration; projective geometry

为了防止发方与收方之间的相互欺骗, SIMMONS 在普通认证码的基础上引入了带仲裁的认证码模型(简记为 $A^2$-码)[1], 此模型涉及发方、收方、敌方以及仲裁 4 个参与方以及 5 种攻击。敌方可对系统进行模仿攻击($\boldsymbol{I}$)和替换攻击($\boldsymbol{S}$), 发方可进行模仿攻击($\boldsymbol{T}$), 收方可进行模仿攻击($\boldsymbol{R}_0$)和替换攻击($\boldsymbol{R}_1$)。关于这 5 种攻击的定义见文献[2], 它们攻击成功的概率分别记为 $\boldsymbol{P}_I$, $\boldsymbol{P}_S$, $\boldsymbol{P}_T$, $\boldsymbol{P}_{R_0}$和 $\boldsymbol{P}_{R_1}$。仲裁了解通信系统的全部但不参与通信活动, 只有当发方与收方发生争端时才出面解决争端, 因此假定仲裁是诚实的。下面给出 $A^2$-码的定义。

定义 **1**　设 $\boldsymbol{S}, \boldsymbol{E}_T, \boldsymbol{E}_R, \overline{\boldsymbol{M}}$ 是 4 个非空的有限集合, $f: \boldsymbol{S} \times \boldsymbol{E}_T \to \overline{\boldsymbol{M}}$, $g: \overline{\boldsymbol{M}} \times \boldsymbol{E}_R \to \boldsymbol{S} \cup \{$欺诈$\}$ 是 2 个映射, 6 元组$(\boldsymbol{S}, \boldsymbol{E}_T, \boldsymbol{E}_R, \overline{\boldsymbol{M}}; f, g)$叫作一个带仲裁的认证码, 如果:

1) $f$, $g$ 是满射;

2) 对任意 $\boldsymbol{M} \in \overline{\boldsymbol{M}}$, $\boldsymbol{E}_T \in \boldsymbol{E}_T$, 若有 $\boldsymbol{S} \in \boldsymbol{S}$ 使得 $f(\boldsymbol{S}, \boldsymbol{E}_T) = \boldsymbol{M}$, 则 $\boldsymbol{S}$ 由 $\boldsymbol{M}$ 和 $\boldsymbol{E}_T$ 唯一确定;

3) 若 $\boldsymbol{P}(\boldsymbol{E}_T, \boldsymbol{E}_R) > 0$ 且 $f(\boldsymbol{S}, \boldsymbol{E}_T) = \boldsymbol{M}$, 则 $g(\boldsymbol{M}, \boldsymbol{E}_R) = \boldsymbol{S}$, 否则 $g(\boldsymbol{M}, \boldsymbol{E}_R)$为欺诈。

分别称 $\boldsymbol{S}, \boldsymbol{E}_T, \boldsymbol{E}_R, \overline{\boldsymbol{M}}$ 为信源集、发方编码规则集、收方编码规则集和信息集, $f$ 与 $g$ 分别叫作编码映射和译码映射, 基数 $|\boldsymbol{S}|$, $|\boldsymbol{E}_T|$, $|\boldsymbol{E}_R|$, $|\overline{\boldsymbol{M}}|$ 称为这个码的参数。

定义 **2**　设 6 元组$(\boldsymbol{S}, \boldsymbol{E}_T, \boldsymbol{E}_R, \overline{\boldsymbol{M}}; f, g)$是 $A^2$-码, 若 $|\boldsymbol{E}_T| = \dfrac{1}{\boldsymbol{P}_I \boldsymbol{P}_S \boldsymbol{P}_{R_0} \boldsymbol{P}_{R_1}}$, $|\boldsymbol{E}_R| = \dfrac{1}{\boldsymbol{P}_I \boldsymbol{P}_S \boldsymbol{P}_T}$, 则称此 $A^2$-码是

收稿日期: 2010-07-12; 修回日期: 2010-10-15; 责任编辑: 张　军

基金项目: 河北省自然科学基金资助项目(A2008000128); 河北省教育厅自然科学基金资助项目(2007127)

作者简介: 张晓寒(1972-), 女, 河北武邑人, 副教授, 硕士, 主要从事代数与代数组合论方面的研究。

完备的。

JOHANSSON 在文献[2]中用射影几何 $PG(3, \boldsymbol{F}_q)$ 构作了2个完备的 $A^2$-码，李瑞虎等在文献[3]中用射影几何 $PG(n, \boldsymbol{F}_q)$, $n \geq 3$ 构作了一类完备的 $A^2$-码，推广了文献[2]中的构作。笔者用射影几何 $PG(n, \boldsymbol{F}_q)$, $n \geq 5$ 构作了一类新的带仲裁的认证码，计算了有关的参数，并证明了它在一定条件下是完备的。

## 1 射影几何的预备知识

设 $n \geq 1$ 为整数，$\boldsymbol{F}_q^{(n+1)}$ 是 $\boldsymbol{F}_q$ 上的 $(n+1)$ 维行向量空间。$\boldsymbol{F}_q^{(n+1)}$ 的一维向量子空间定义为点，$\boldsymbol{F}_q^{(n+1)}$ 的2维、3维、$n$ 维向量子空间分别定义为线、面和超平面。更一般的，$\boldsymbol{F}_q^{(n+1)}$ 的 $(r+1)$ 维子空间定义为射影 $r$-面。若一个射影 $r$-面作为向量子空间来说包含或被包含于一个作为射影 $s$-面的向量子空间，则称这2个面是关联的。那么点集，即 $\boldsymbol{F}_q^{(n+1)}$ 的一维向量子空间集，与 $r(0 \leq r \leq n)$-面及其上的关联关系称为 $\boldsymbol{F}_q$ 上的 $n$ 维射影空间，记为 $PG(n, \boldsymbol{F}_q)$。

由文献[4]可知下面的命题成立。

命题 **1** 设 $0 \leq r \leq n$，用 $\boldsymbol{P}$ 表示 $PG(n, \boldsymbol{F}_q)$ 中的 $r$-面，用 $\boldsymbol{P}$ 表示与之相对应的 $\boldsymbol{F}_q^{(n+1)}$ 中的 $(r+1)$ 维子空间，则 $\boldsymbol{P} \subseteq \boldsymbol{P}$ 是 $PG(n, \boldsymbol{F}_q)$ 中 $r$-面的集合到 $\boldsymbol{F}_q^{(n+1)}$ 中 $(r+1)$ 维子空间集合的一个一一对应关系。

由文献[5]对于 $\boldsymbol{F}_q^{(n)}$ 的向量子空间可知下面的命题成立。

命题 **2** 设 $m, s$ 是2个正整数，且 $\max\{0, m+s-n\} \leq t \leq \min\{m, s\}$，$\boldsymbol{P}$ 是向量空间 $\boldsymbol{F}_q^{(n)}$ 中任一个 $m$ 维子空间，$\boldsymbol{F}_q^{(n)}$ 中满足 $\dim(\boldsymbol{P} \cap \boldsymbol{R}) = t$ 的 $s$ 维子空间 $\boldsymbol{R}$ 的个数等于 $q^{(s-t)(m-t)} \begin{bmatrix} n-m \\ s-t \end{bmatrix}_q \begin{bmatrix} m \\ t \end{bmatrix}_q$。

由命题2易得下面的推论。

推论 **1** 设 $m, s$ 是2个正整数，且 $\max\{0, m+s-n\} \leq t \leq \min\{m, s\}$，$\boldsymbol{P}$ 是向量空间 $\boldsymbol{F}_q^{(n)}$ 中任一个 $m$ 维子空间，$\boldsymbol{U}$ 是 $\boldsymbol{P}$ 中一个固定的 $t$ 维子空间。$\boldsymbol{F}_q^{(n)}$ 中满足 $\boldsymbol{P} \cap \boldsymbol{R} = \boldsymbol{U}$ 的 $s$ 维子空间 $\boldsymbol{R}$ 的个数等于

$$q^{(s-t)(m-t)} \begin{bmatrix} n-m \\ s-t \end{bmatrix}_q.$$

在以下的叙述中，笔者用同样的字母来表示 $PG(n, \boldsymbol{F}_q)$ 中的 $r$-面和与之相对应的 $\boldsymbol{F}_q^{(n+1)}$ 中的 $(r+1)$ 维子空间。

## 2 $A^2$-码的构作

设 $2 < r < r_0 < n$，$\boldsymbol{U}$ 是 $\boldsymbol{F}_q^{(n+1)}$ 中一个固定的2维子空间，$\boldsymbol{P}_0$ 为包含 $\boldsymbol{U}$ 的 $r_0$ 维子空间，则定义

$$\boldsymbol{S} = \{\boldsymbol{S} \mid \boldsymbol{S} \text{为} r \text{维子空间}, \boldsymbol{U} \subseteq \boldsymbol{S} \subseteq \boldsymbol{P}_0\}, \boldsymbol{E}_T = \{\boldsymbol{E}_T \mid \boldsymbol{E}_T \text{为3-面}, \boldsymbol{E}_T \cap \boldsymbol{P}_0 = \boldsymbol{U}\},$$

$$\boldsymbol{E}_R = \{\boldsymbol{E}_R \mid \boldsymbol{E}_R \text{为2-面}, \boldsymbol{E}_R \cap \boldsymbol{P}_0 = \boldsymbol{U}\}, \overline{\boldsymbol{M}} = \{\boldsymbol{M} \mid \boldsymbol{M} \text{为}(r+1)\text{-面}, \boldsymbol{M} \cap \boldsymbol{P}_0 \subseteq \boldsymbol{S}\},$$

并定义 $f: \boldsymbol{S} \times \boldsymbol{E}_T \to \overline{\boldsymbol{M}}$，$(\boldsymbol{S}, \boldsymbol{E}_T) \to \boldsymbol{M} = \boldsymbol{S} \cup \boldsymbol{E}_T$，$g: \overline{\boldsymbol{M}} \times \boldsymbol{E}_R \to \boldsymbol{S} \cup \{\text{欺诈}\}$。

若 $\boldsymbol{E}_R \subseteq \boldsymbol{M}$，则 $(\boldsymbol{M}, \boldsymbol{E}_R) \to \boldsymbol{S}$，其中 $\boldsymbol{S} = \boldsymbol{M} \cap \boldsymbol{P}_0$，否则 $(\boldsymbol{M}, \boldsymbol{E}_R) \to \{\text{欺诈}\}$。

引理 **1** 1) $\boldsymbol{S} \subseteq \boldsymbol{S}, \boldsymbol{E}_T \to \boldsymbol{E}_T$，则 $\boldsymbol{S} \cup \boldsymbol{E}_T$ 是一个信息。2) $\boldsymbol{M} \in \overline{\boldsymbol{M}}$，则 $\boldsymbol{S} = \boldsymbol{M} \cap \boldsymbol{P}_0$ 是包含于 $\boldsymbol{P}_0$ 的唯一信源。

证 明 1) 由 $\dim(\boldsymbol{S} \cap \boldsymbol{E}_T) + \dim(\boldsymbol{S} \cup \boldsymbol{E}_T) = \dim \boldsymbol{S} + \dim \boldsymbol{E}_T$ 可知，

$\dim(\boldsymbol{S} \cap \boldsymbol{E}_T) = \dim \boldsymbol{S} + \dim \boldsymbol{E}_T - \dim(\boldsymbol{S} \cup \boldsymbol{E}_T) = r+2$，故 $\boldsymbol{S} \cup \boldsymbol{E}_T$ 是一个信息。

2) 设另有 $\boldsymbol{S}'$，使 $\boldsymbol{S}' \cup \boldsymbol{E}_T = \boldsymbol{M}$，则 $\boldsymbol{S}' \subseteq (\boldsymbol{M} \cap \boldsymbol{P}_0)$，由维数关系 $\boldsymbol{S}' = \boldsymbol{M} \cap \boldsymbol{P}_0 = \boldsymbol{S}$，唯一性得证。

定理 **1** 上述构作是一个 $A^2$-码。

证 明 1) $f$，$g$ 是满射。

首先证 $f$ 是满射。由引理1中的1)可知，$f$ 已是映射。设 $\boldsymbol{M}$ 是一个信息，则 $\boldsymbol{M} \cap \boldsymbol{P}_0 = \boldsymbol{S}$ 是一个信源，由于 $\dim \boldsymbol{M} = r+2 > \dim \boldsymbol{S} = r$，在 $\boldsymbol{M}$ 中存在一个2维子空间 $\boldsymbol{Q}$ 使得 $\boldsymbol{Q} \cap \boldsymbol{P}_0 = \{0\}$，于是 $\boldsymbol{E}_T = \boldsymbol{Q} \cup \boldsymbol{U}$ 是一个4维子空间(3-面)且 $\boldsymbol{E}_T \cap \boldsymbol{P}_0 = \boldsymbol{U}$，也就是说 $\boldsymbol{E}_T$ 是一个发方编码规则，且 $\boldsymbol{S} \cup \boldsymbol{E}_T = \boldsymbol{M}$，因此 $f$ 是满射。

再证 $g$ 是满射。$g$ 显然是一个映射。任取一个信源 $\boldsymbol{S}$，必有一个信息 $\boldsymbol{M}$ 使得 $\boldsymbol{M} \cap \boldsymbol{P}_0 = \boldsymbol{S}$，由于 $\dim \boldsymbol{M} = r+2 > \dim \boldsymbol{S} = r$，所以必存在一个一维子空间 $\boldsymbol{W} \subseteq \boldsymbol{M}$，但是 $\boldsymbol{W} \cap \boldsymbol{P}_0 = \{0\}$，这样 $\boldsymbol{W} \cup \boldsymbol{U} = \boldsymbol{E}_R$ 是一个2-面，$\boldsymbol{E}_R \cap \boldsymbol{P}_0 = \boldsymbol{U}$，即 $\boldsymbol{E}_R$ 是一个收方编码规则，且 $\boldsymbol{E}_R \subseteq \boldsymbol{M}$，故 $g$ 是满射。

2) 由引理 1 中的 2) 可知 $S$ 由 $M$ 和 $E_T$ 唯一确定。

3) 若 $P(E_T, E_R)$　0( 即 $E_R$　$E_T$) 且 $f(S, E_T) = M$, 由 $M = S$　$E_T$, 知 $E_R$　$M$, 因此 $g(M, E_R) = S$, 否则 $g(M, E_R) = \{$欺诈$\}$。

**定理 2**　上述构作所得 $A^2$-码具有以下参数:

$$|S| = \begin{bmatrix} r_0 - 2 \\ r - 2 \end{bmatrix}_q, |E_T| = q^{2(r_0-2)} \begin{bmatrix} n + 1 - r_0 \\ 2 \end{bmatrix}_q, |E_R| = q^{r_0-2} \begin{bmatrix} n + 1 - r_0 \\ 1 \end{bmatrix}_q, |\overline{M}| = q^{2(r_0-r)} \begin{bmatrix} n + 1 - r_0 \\ 2 \end{bmatrix}_q \begin{bmatrix} r_0 \\ r \end{bmatrix}_q 。$$

证　明　1) 因为 $U$　$S$　$P_0$, 由文献[4]易得 $|S| = \begin{bmatrix} r_0 - 2 \\ r - 2 \end{bmatrix}_q$。

2) $|E_T|$ 即是与 $P_0$ 相交于子空间 $U$ 的 4 维子空间的个数, 由推论 1 可得:

$$|E_T| = q^{2(r_0-2)} \begin{bmatrix} n + 1 - r_0 \\ 2 \end{bmatrix}_q 。$$

3) $|E_R|$ 的求法与 2) 类似。

4) $|\overline{M}|$ 即为与 $P_0$ 相交于 $r$ 维子空间的 $(r + 2)$ 维子空间的个数, 由命题 2 可得:

$$|\overline{M}| = q^{2(r_0-r)} \begin{bmatrix} n + 1 - r_0 \\ 2 \end{bmatrix}_q \begin{bmatrix} r_0 \\ r \end{bmatrix}_q 。$$

**引理 2**　1) 任取 $E_T$　$E_T$, $E_T$ 所包含的 $E_R$ 的个数为 $c = \dfrac{q^2 - 1}{q - 1}$。

2) 任取 $E_R$　$E_R$, 包含 $E_R$ 的 $E_T$ 的个数为 $d = \dfrac{q^{r_0-2}(q^{n-r_0} - 1)}{q - 1}$。

证　明　1) 因为 $U$　$(E_T$　$E_R)$, 又 $E_T$ 包含 $E_R$, $c$ 相当于包含在一个给定 2 维空间中的 1 维子空间的个数, 易得:

$$c = \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q = \frac{q^2 - 1}{q - 1} 。$$

2) 因为 $U$　$(E_T$　$E_R)$, $d$ 相当于求包含一个给定 3 维空间 $E_R$ 的满足 $E_T$　$P_0 = U$ 的 4 维子空间的 $E_T$ 的个数。由于一般线性群可迁地作用在同维子空间的集合上, 这样可以设:

$$U = (e_1, e_2)^{\mathrm{T}}, E_R = (e_1, e_2, e_3)^{\mathrm{T}}, P_0 = (e_1, e_2, e_4, \quad , e_{r_0}, e_{r_0+1})^{\mathrm{T}} 。$$

于是, 满足条件的子空间 $E_T$ 的矩阵表示具有下面的形式:

$$E_T = \begin{matrix} 3 & r_0 - 2 & n - r_0 \end{matrix} \\ \begin{pmatrix} I^{(3)} & 0 & 0 \\ 0 & v_1 & v_2 \end{pmatrix} \begin{matrix} 3 \\ 1 \end{matrix},$$

其中: $v_1$ 是任意的 $(r_0 - 2)$ 维行向量; $v_2$ 是不为零的 $(n - r_0)$ 维行向量, 故经简单计算可得:

$$d = q^{r_0-2} \begin{bmatrix} n - r_0 \\ 1 \end{bmatrix}_q = \frac{q^{r_0-2}(q^{n-r_0} - 1)}{q - 1} 。$$

**引理 3**　任取 $M$　$\overline{M}$ 及 $E_R$　$M$, 则有: 1) $M$ 中包含 $E_R$ 的 $E_T$ 的个数为 $q^{r-2}$; 2) $M$ 中包含的 $E_R$ 的个数为

$$q^{r-2} \frac{q^2 - 1}{q - 1} = q^{r-2}(q + 1) 。$$

证　明　1) 由题意得 $E_R$　$E_T$　$M$, 不妨设 $U = (e_1, e_2)^{\mathrm{T}}$, $E_R = (e_1, e_2, e_3)^{\mathrm{T}}$, $P_0 = (e_1, e_2, e_4, \quad , e_{r_0}, e_{r_0+1})^{\mathrm{T}}$, $M = (e_1, e_2, e_3, e_4, \quad , e_r, e_{r_0+1}, e_{r_0+2})^{\mathrm{T}}$。

于是, 满足条件的子空间 $E_T$ 的矩阵表示具有下面的形式:

$$E_T = \begin{matrix} 3 & r - 3 & r_0 - r & 1 & 1 & n - r_0 - 1 \end{matrix} \\ \begin{pmatrix} I^{(3)} & 0 & 0 & 0 & 0 & 0 \\ 0 & v_1 & 0 & v_2 & 1 & 0 \end{pmatrix} \begin{matrix} 3 \\ 1 \end{matrix},$$

其中: $v_1$ 是任意的 $(r - 3)$ 维行向量; $v_2$ 是 $F_q$ 中的任意元素, 故易得所求个数为 $q^{r-2}$。

2) 用同 1) 类似的方法计算即得。

**引理 4**　若 $M_1$ 与 $M_2$ 是共同包含发方的一个编码规则 $E_T$ 的 2 个不同信息, $S_1$ 与 $S_2$ 分别为 $M_1$ 与 $M_2$ 包含的信源, 设 $S_0 = S_1$　$S_2$, $\dim S_0 = k$, 则 2　$k$　$r - 1$, 并且有如下成立。

1) $\boldsymbol{M}_1 \cap \boldsymbol{M}_2$ 所包含的 $\boldsymbol{E}_R$ 数为 $q^{k-2}\dfrac{q^2-1}{q-1}=q^{k-2}(q+1)$。

2) 任取 $\boldsymbol{E}_R \subset (\boldsymbol{M}_1 \cap \boldsymbol{M}_2)$, $\boldsymbol{M}_1 \cap \boldsymbol{M}_2$ 中包含 $\boldsymbol{E}_R$ 的 $\boldsymbol{E}_T$ 的个数为 $q^{k-2}$。

证 明 $\dim(\boldsymbol{M}_1 \cap \boldsymbol{M}_2)=\dim(\boldsymbol{S}_1 \cap \boldsymbol{S}_2)+\dim \boldsymbol{E}_T-\dim(\boldsymbol{S}_1 \cap \boldsymbol{S}_2 \cap \boldsymbol{E}_T)=k+4-2=k+2$, 因为 $\boldsymbol{M}_1 \cap \boldsymbol{M}_2 \cap \boldsymbol{E}_R=U$, $\dim(\boldsymbol{M}_1 \cap \boldsymbol{M}_2 \cap \boldsymbol{P}_0)=\dim(\boldsymbol{S}_1 \cap \boldsymbol{S}_2)=k$, 用和引理 3 同样的方法可得。

定理 **3** 在构作所得的 $A^2$–码中, 若编码规则按等概率分布选取, 则各种攻击成功的概率分别如下:

$$\boldsymbol{P}_I=\frac{q^2-1}{q^{r_0-r}(q^{n+1-r_0}-1)},\ \boldsymbol{P}_S=\frac{1}{q},\ \boldsymbol{P}_T=\frac{q-1}{q^2-1},\ \boldsymbol{P}_{R_0}=\frac{q-1}{q^{r_0-r}(q^{n-r_0}-1)},\ \boldsymbol{P}_{R_1}=\frac{1}{q}。$$

证 明 1) 设敌方用信息 $\boldsymbol{M}$ 欺骗收方, 模仿攻击成功当且仅当 $\boldsymbol{M}$ 包含收方编码规则集。由于 $\boldsymbol{M}$ 包含的 $\boldsymbol{E}_R$ 个数是 $q^{r-2}\begin{bmatrix}2\\1\end{bmatrix}_q$, 而 $\boldsymbol{E}_R$ 的总数为 $|\boldsymbol{E}_R|=q^{r_0-2}\begin{bmatrix}n+1-r_0\\1\end{bmatrix}_q$, 故

$$\boldsymbol{P}_I=\frac{q^{r-2}\begin{bmatrix}2\\1\end{bmatrix}_q}{q^{r_0-2}\begin{bmatrix}n+1-r_0\\1\end{bmatrix}_q}=\frac{q^2-1}{q^{r_0-r}(q^{n+1-r_0}-1)}。$$

2) 设敌方截获发方发送的信息 $\boldsymbol{M}_1$, 而用 $\boldsymbol{M}_2$ 替换后发给收方。只有当 $\boldsymbol{M}_1$ 包含的信源 $\boldsymbol{S}_1$ 与 $\boldsymbol{M}_2$ 包含的信源 $\boldsymbol{S}_2$ 不同时, 其替换攻击才可能成功。由于 $\boldsymbol{E}_R \subset \boldsymbol{E}_T \subset \boldsymbol{M}_1$, 故敌方的最优策略是选取 $\boldsymbol{E}_T \subset \boldsymbol{P}_1$, 使 $\boldsymbol{P}_2=\boldsymbol{S}_2 \cup \boldsymbol{E}_T$, 且 $r=\dim(\boldsymbol{S}_1 \cap \boldsymbol{S}_2)$ 尽可能大。由于 $\boldsymbol{M}_1 \cap \boldsymbol{M}_2$ 所包含的 $\boldsymbol{E}_R$ 个数为 $q^{k-2}(q+1)$, 而 $\boldsymbol{M}$ 包含的 $\boldsymbol{E}_R$ 个数是 $q^{r-2}(q+1)$, 故 $\boldsymbol{P}_S=\max\limits_k \dfrac{q^{k-2}(q+1)}{q^{r-2}(q+1)}$, 当 $k=r-1$ 时, $\boldsymbol{P}_S$ 最大, 为 $\dfrac{1}{q}$。

3) 设发方发送 1 个信息 $\boldsymbol{M}$ 给收方, $\boldsymbol{M}$ 不包含发方自己的编码规则 $\boldsymbol{E}_T$; 信息 $\boldsymbol{M}$ 被收方接受当且仅当 $\boldsymbol{M}$ 包含收方的编码规则 $\boldsymbol{E}_R$。由于 $\boldsymbol{E}_R \subset \boldsymbol{E}_T$, 故发方要选取 $\boldsymbol{M}$ 使 $\boldsymbol{M}$ 包含尽可能多的 $\boldsymbol{E}_R(\boldsymbol{E}_R \subset \boldsymbol{E}_T)$ 且 $\boldsymbol{E}_T$ 不包含在 $\boldsymbol{M}$ 中, 由维数公式可以断言这样的信息 $\boldsymbol{M}$ 至多包含 1 个含于 $\boldsymbol{E}_T$ 的 $\boldsymbol{E}_R$, 故 $\boldsymbol{P}_T=\dfrac{1}{\begin{bmatrix}2\\1\end{bmatrix}_q}=\dfrac{q-1}{q^2-1}$。

4) 设收方声称收到信息 $\boldsymbol{M}$, 若 $\boldsymbol{M}$ 包含发方的编码规则 $\boldsymbol{E}_T$, 则收方的模仿攻击成功。因收方知道 $\boldsymbol{E}_R \subset \boldsymbol{E}_T$, 故收方要选取 $\boldsymbol{M}$, 使 $\boldsymbol{M} \cap \boldsymbol{E}_R$; 由于 $\boldsymbol{M}$ 中包含 $\boldsymbol{E}_R$ 的 $\boldsymbol{E}_T$ 的个数为 $q^{r-2}$(引理 3), 而包含 $\boldsymbol{E}_R$ 的 $\boldsymbol{E}_T$ 总数为 $d=q^{r_0-2}\begin{bmatrix}n-r_0\\1\end{bmatrix}_q$(引理 2), 故 $\boldsymbol{P}_{R_0}=\dfrac{q^{r-2}}{q^{r_0-2}\begin{bmatrix}n-r_0\\1\end{bmatrix}_q}=\dfrac{q-1}{q^{r_0-r}(q^{n-r_0}-1)}$。

5) 设收方收到信息 $\boldsymbol{M}_1$ 后却声称收到的是 $\boldsymbol{M}_2$, 只有当 $\boldsymbol{M}_1$ 包含的信源 $\boldsymbol{S}_1$ 与 $\boldsymbol{M}_2$ 包含的信源 $\boldsymbol{S}_2$ 不同时, 其替换攻击才可能成功。由于 $\boldsymbol{E}_R \subset \boldsymbol{E}_T \subset \boldsymbol{M}$, 故敌方的最优策略是选取 $\boldsymbol{P}_2=\boldsymbol{S}_2 \cup \boldsymbol{E}_T$, 其中 $\boldsymbol{E}_R \subset \boldsymbol{E}_T \subset \boldsymbol{M}_1$, 且 $r=\dim(\boldsymbol{S}_1 \cap \boldsymbol{S}_2)$ 尽可能大。由于 $\boldsymbol{M}_1 \cap \boldsymbol{M}_2$ 中包含 $\boldsymbol{E}_R$ 的 $\boldsymbol{E}_T$ 的个数为 $q^{k-2}$(引理 4), 而 $\boldsymbol{M}$ 中包含 $\boldsymbol{E}_R$ 的 $\boldsymbol{E}_T$ 的个数为 $q^{r-2}$(引理 3), 故 $\boldsymbol{P}_{R_1}=\max\limits_k \dfrac{q^{k-2}}{q^{r-2}}$, 当 $k=r-1$ 时达到最大值, 为 $\dfrac{1}{q}$。

由定理 2 和定理 3 易知这个构作当 $r=3$ 时是完备的 $A^2$–码。

参考文献:


[1] SIMMONS G J. Message authentication with arbitration of transmitter/receiver disputes[A]. Chaum D Price W L. Proc Eurocrypt 87[C]. Berlin: Springer Verlag, 1988. 151-165.

[2] JOHANSSON T. Lower bounds on the probability of deception in authentication with arbitration[J]. IEEE Transactions on Information Theory, 1994, 40(5): 1 573-1 585.

[3] 李瑞虎, 李尊贤. 利用射影几何构作一类完备的 $A^2$–码[J]. 通信保密(Communications Privacy), 1997, 37(3): 72-76.

[4] WAN Zhe-xian. Geometry of Classical Groups over Finite Fields[M]. 2nd Ed. Beijing/New York: Science Press, 2002. 61-106.

[5] 郭 军, 霍元极, 赵东明. 有限向量空间中子空间的计数公式及其应用[J]. 河北师范大学学报(Journal of Hebei Normal University(Natural Science Edition)), 2004, 28(6): 561-564.

[6] SIMMONS G J. Authentication theory/coding theory[A]. Advances in Cryptology-Crypto'84, Lecture Notes in Computer Science 196[C]. Berlin: Springer-Verlag, 1985. 411-431.

[7] 李 莉, 霍丽君, 李志梅. 辛几何上具有仲裁的认证码的一类新构作[J]. 河北科技大学学报(Journal of Hebei University of Science and Technology), 2010, 31(4): 294-299.