# 利用酉几何进一步构造带仲裁的认证码 [1]

李瑞虎 * ** 李志慧 * 李学良 *

*(西北工业大学应用数学系 西安 710072)
**(空军工程大学导弹学院数学教研室 陕西三原 713800)

**摘 要** 该文利用有限域上的酉几何构作了三类新的带仲裁的认证码，计算了码的参数；当编码规则按等概率分布选取时，计算出各种攻击成功的概率．研究结果表明可用酉几何进一步构作多类带仲裁的认证码．

**关键词** 有限域，酉几何，认证码，仲裁
**中图号** TN918.1

## 1 引 言

为解决通信系统中发方与收方互不信任问题， G. J. Simmons[1] 在普通认证码的基础上引入带仲裁的认证码的模型，以下简称为 $A^2$-码。在这个模型中有 4 个参与者：发方、收方、敌方和仲裁。敌方可对系统进行模仿攻击 $(I)$ 和替换攻击 $(S)$，发方可进行模仿攻击 $(T)$，收方可进行模仿攻击 $(R_0)$ 和替换攻击 $(R_1)$(关于这 5 种攻击的定义见文献 [1,2])；这 5 种攻击成功的概率分别记为 $P_I$, $P_S$, $P_T$, $P_{R_0}$ 和 $P_{R_1}$。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执时才出面解决争端，因此假定仲裁者总是诚实的。

设 $\varsigma$, $\xi_T$, $\xi_R$ 和 $\chi$ 为 4 个非空有限集合， $f:\varsigma\times\xi_T\to\chi$ 和 $g:\chi\times\xi_R\to\varsigma\cup\{$欺诈$\}$ 为两个映射，六元组 $(\varsigma,\xi_T,\xi_R,\chi;f,g)$ 叫做一个 $A^2$-码。如果这个六元组满足：

(1) $f$ 与 $g$ 为满射；

(2) $\forall M\in\chi, E_T\in\xi_T$，如果存在 $S\in\varsigma$ 使得 $f(S,E_T)=M$ 则这样的 $S$ 由 $M$ 和 $E_T$ 唯一确定。

(3) 若 $P(E_T,E_R)\neq 0$ 且 $f(S,E_T)=M$，则 $g(M,E_R)=S$，否则 $g(M,E_R)=$欺诈。

在此 $A^2$-码中，集合 $\varsigma,\xi_T,\xi_R$ 和 $\chi$ 分别叫信源集、发方的编码规则集、收方的译码规则集和信息集； $f$ 与 $g$ 分别叫编码映射和译码映射。基数 $|\varsigma|$, $|\xi_T|$, $|\xi_R|$ 和 $|\chi|$ 叫做这个码的参数。

对本文以下构做的 $A^2$-码，约定每次认证通信是发方采用的秘密编码规则 $E_T$ 和收方采用的译码规则 $E_R$ 具有关系 $E_T\supset E_R$。通信过程中 $E_T$ 与 $E_R$ 的选取办法以及认证方法见文献 [2, 3]。文献 [2, 3] 用有限域上酉几何构做 $A^2$ 码，得到了较好的结果。本文在文献 [4–7] 研究的基础上，利用酉几何构做三类新的 $A^2$-码，为此先介绍有关酉几何的预备知识。

## 2 酉几何

设 $F_{q^2}$ 是 $q^2$ 元有限域，其中 $q$ 为素数的幂。$F_{q^2}$ 有一对合自同构 $\sigma:a\mapsto\overline{a}=a^q$, $\sigma$ 的固定子域是 $F_q$。设 $n=2\gamma+\delta$, $\delta=0$ 或 1，令 $H_{2\gamma+\delta}$ 为 $H_{2\gamma}=\begin{pmatrix}0 & I^{(\gamma)}\\ I^{(\gamma)} & 0\end{pmatrix}$, $H_{2\gamma+1}=\begin{pmatrix}H_{2\gamma} & 0\\ 0 & 1\end{pmatrix}$。

以 $V_n(F_{q^2})$ 表示 $F_{q^2}$ 上 $n$ 维行向量空间，群 $U_n(F_{q^2})=\{T\in GL_n(F_{q^2})|TH_n\overline{T}^T=H_n\}$ 叫做 $F_{q^2}$ 上关于 $H_n$ 的 $n$ 阶酉群。规定 $U_n(F_{q^2})$ 在 $V_n(F_{q^2})$ 上的作用如下：

$$V_n(F_{q^2})\times U_n(F_{q^2})\to V_n(F_{q^2}),((x_1,x_2,\cdots,x_n),T)\mapsto(x_1,x_2,\cdots,x_n)T$$

带有上述酉群作用的 $n$ 维行向量空间 $V_n(F_{q^2})$ 叫做 $F_{q^2}$ 上的 $n$ 维酉空间。

[1] 2000-07-10 收到， 2001-05-09 定稿
西北工业大学博士创新基金资助项目

设 $P$ 是 $V_n(F_{q^2})$ 的一个 $m$ 维子空间，并用同样字母 $P$ 表示该子空间的任一矩阵，即 $P$ 的行构成该子空间的一组基；如果 $PH_n\overline{P}^T$ 的秩为 $r$，就称 $P$ 是一个 $(m,r)$ 型子空间．由文献 [8] 可知 $V_n(F_{q^2})$ 的同型子空间构成在 $U_n(F_{q^2})$ 作用下的一条轨道．

设 $P$ 是 $V_n(F_{q^2})$ 的任一子空间，其对偶子空间记为 $P^\perp$，即

$$P^\perp = \{x \in V_n(F_{q^2}) | xH_n\overline{y}^T = 0, \quad \forall y \in P\}$$

则当 $P$ 为 $(m,r)$ 型子空间时，$P^\perp$ 为 $(n-m, n-2m+r)$ 型子空间．

以 $N(m,r;n)$ 表示 $V_n(F_{q^2})$ 中 $(m,r)$ 型子空间的个数，以 $N(m_1,r_1;m,r;n)$ 表示 $V_n(F_{q^2})$ 中一个 $(m,r)$ 型子空间所包含的 $(m_1,r_1)$ 型子空间的个数，而以 $N'(m_1,r_1;m,r;n)$ 表示 $V_n(F_{q^2})$ 中包含某一 $(m_1,r_1)$ 型子空间的 $(m,r)$ 型子空间的个数；关于 $N(m,r;n)$、$N(m_1,r_1;m,r;n)$ 的详细公式见文献 [8]．以 $N(k,s)$ 表示 $V_n(F_{q^2})$ 中一个 $s$ 维子空间所包含的 $k$ 维子空间个数，当 $k \le s$ 时，$N(k,s) = \prod_{i=s-k+1}^{s}(q^{2i}-1)/\prod_{i=1}^{k}(q^{2i}-1)$．

**3 构作 (1)**

设 $n = 2\gamma + \delta$，$1 < s_1 < s < \gamma$；固定 $U$ 为 $V_n(F_{q^2})$ 的一个 $(s,0)$ 型子空间，则 $U^\perp$ 为 $(n-2, n-2s)$ 型子空间．定义 $V_n(F_{q^2})$ 的如下子空间所构成的集合：

$\varsigma = \{S | S$为$(n-2s, n-2s)$ 型子空间，$S \subset U^\perp\}$

$\xi_T = \{E_T | E_T$为 $s$ 维子空间$, U + E_T$为 $(2s, 2s)$ 型子空间$\}$

$\xi_R = \{E_R | E_R$为 $s_1$ 维子空间$, U + E_R$为 $(s+s_1, 2s_1)$ 型子空间$\}$

$\chi = \{M | M$为 $n-s$ 维子空间$, M^\perp \in \xi_T\}$

并定义

$f : \varsigma \times \xi_T \to \chi, \quad (S, E_T) \mapsto M = S + E_T$

$g : \chi \times \xi_R \to \chi \cup \{$欺骗$\}$

$$(M, E_R) \mapsto \begin{cases} S & \text{若 } E_R \subset M, \quad \text{其中 } S = M \cap U^\perp \\ \text{欺骗} & \text{若 } E_R \not\subset M \end{cases}$$

利用文献 [4] 的引理 1 易验证 $(\varsigma, \xi_T, \xi_R, \chi, f, g)$ 是一个 $A^2$–码．

为叙述简便，下文用 $S$, $E_T$, $E_R$ 和 $M$ 分别表示任意信源，发方的编码规则，收方的译码规则和信息．仿照文献 [2,4] 易验证下述结论成立．

**引理 1**　$\forall M \in \chi$，则 $M$ 包含的 $E_T$ 及 $E_R$ 的个数分别为 $q^{2s(n-2s)}$ 和 $q^{2s_1(n-2s)}N(s_1,s)$．

利用引理 1 和文献 [4] 的定理 1 可证明．

**定理 1**　构作 1 所得 $A^2$–码具有参数

$$|\varsigma| = q^{2s(2\gamma-2s+\delta)} = q^{2s(n-2s)}, \ |\xi_T| = |\chi| = q^{2s(2\gamma-s+\delta)} = q^{2s(n-s)}, \ |\xi_R| = N(s_1,s) = q^{2s_1(n-2s)}$$

**引理 2**　(1) $\forall E_T$ 包含的 $E_R$ 个数为 $N(s_1,s)$; (2) $\forall E_R \in \xi_R$，则包含 $E_R$ 的 $E_T$ 个数为 $q^{2(s-s_1)(n-s)}$．

**引理 3**　$\forall M \in \chi$ 及 $\forall E_R \subset M$，则 $M$ 中包含 $E_R$ 的 $E_T$ 的个数为 $q^{2(s-s_1)(n-2s)}$．

**引理 4**　设 $M_1$ 与 $M_2$ 是共同含发方的某一编码规则 $E_T'$ 的两个不同信息，$S_1$ 与 $S_2$ 分别为 $M_1$ 与 $M_2$ 包含的信源．记 $\dim(S_1 \cap S_2) = k$，则 $2 \le k < n-2s$；并且 $\forall M_1$ 可选取 $M_2$ 使 $k$ 达到 $n-2s-1$．更进一步有

(1) $M_1 \cap M_2$ 包含的 $E_R$ 个数为 $N(s_1,s)q^{2s_1k}$

(2) 若 $E_R \subset M_1 \cap M_2$，则 $M_1 \cap M_2$ 中包含 $E_R$ 的 $E_T$ 个数为 $q^{2(s-s_1)k}$．

由以上引理和定理 1，可得

**定理 2** 若构作 (1) 所得 $A^2$–码中，发方的编码规则和收方的译码规则都按等概率分布选取，则各种攻击成功的概率为

$$P_I = 1/q^{2ss_1},\ P_s = 1/q^{2s_1}, P_T = 1/(q^{2s}-1), P_{R_0} = 1/q^{2s(s-s_1)}, P_{R_1} = 1/q^{2(s-s_1)}$$

## 4 构作 (2)

设 $n = 2\gamma + \delta$, $\delta = 0$ 或 1； $2 < r < r_0 \le \gamma - 2$。固定 $U =< u_1, u_2 >$ 为 $V_n(F_q^2)$ 的一个 $(2,0)$ 型子空间及 $P_0$ 为包含 $U$ 的 $(2r_0, 2r_0)$ 型子空间. 定义 $V_n(F_q^2)$ 的如下子空间集合：

$|\varsigma| = \{S | S$为$(2r,2r)$型子空间$, U \subset S \subset P_0\}$

$|\xi_T| = \{E_T | E_T$为$(4,4)$型子空间$, E_T \cap P_0 = U\}$

$|\xi_R| = \{E_R | E_R$为$(3,2)$型子空间$, E_R \cap P_0 = U\}$

$|\chi| = \{M | M$为$2r+2$维子空间$, M \cap P_0 \in \varsigma\}$

再定义 $f : \varsigma \times \xi_T \to \chi, (S, E_T) \mapsto M = S + E_T$,

$g : \chi \times \xi_R \to \varsigma \cup \{$欺骗$\}$

$$(M, E_R) \mapsto \begin{cases} S, & \text{若 } E_R \subset M, \text{ 其中 } S = M \cap P_0 \\ \text{欺骗}, & \text{若 } E_R \not\subset M \end{cases}$$

仿照文献 [5] 的引理 19 易验知 $(\varsigma, \xi_T, \xi_R, \chi; f, g)$ 是一个 $A^2$–码。并可得到如下两定理.

**定理 3** 构作 (2) 所得的 $A^2$–码具有参数：

$$|\varsigma| = N(2r, 2r; 2r_0), \qquad |\xi_T| = q^{\delta(r_0-2)}(q^{2(n-2r_0)}-1)(q^{2(n-2r_0)}-q^2)$$
$$|\xi_R| = (q^2+1)q^{4(r_0-2)}(q^{2(n-2r_0)}-1), \quad |\chi| = |\varsigma||\xi_T|/q^{8(r-2)}$$

**定理 4** 在构作 (2) 所得 $A^2$–码中，若发方的编码规则和收方的译码规则都按等概率选取，则各种攻击成功的概率分别为

$$P_I = 1/[q^{4(r_0-r)}(q^{2(n-2r_0)}-1)], \quad P_S = 1/q^2, \quad P_T = 1/(q^2+1)$$
$$P_{R_0} = 1/[q^{4(r_2-r)}(q^{2(n-2r_0)}-q^2)], \qquad P_{R_1} = 1/q^2$$

## 5 构作 (3)

设 $n = 2v + \delta$ 及 $U =< u_1, u_2 >$ 如构作 (2) 所述；令 $2r_0 \le 2m_0 \le n + r_0$, $2(r-1) \le r_0 \le 2(m_0 - r_0 - 2)$，固定 $P_0$ 为 $V_n(F_{q^2})$ 中包含 $U$ 的 $(m_0, r_0)$ 型子空间，且 $U \subset P_0 \subset U^T$。定义：

$\varsigma = \{S | U \subset S \subset P_0\}$,其中 $S$ 为 $(2r+1, 2r-2)$ 型子空间

$\xi_T = \{E_T | E_T \cap P_0 = U,$其中 $E_T$ 为 $(4,4)$ 型子空间$\}$

$\xi_R = \{E_R | E_R \cap P_0 = U,$其中 $E_R$ 为 $(3,2)$ 型子空间$\}$

$\chi = \{M | M \cap P_0 = S,\ \mathrm{rank} \cup H_n \overline{M}^T = 2$，其中 $M$ 为 $(2r+3, 2r+2)$ 型子空间 $\}$

再定义 $f : \varsigma \times \xi_T \to \chi, (S, E_T) \mapsto M = S + E_T; \chi \times \xi_T \to \varsigma \cup \{$欺诈$\}$，

$g : (M, E_R) \mapsto S$, 若 $E_R \subset M$, 其中 $S = M \cap P_0$; $(M, E_R) \mapsto$ 欺诈，若 $E_R \not\subset M$。

由文献 [6] 的引理 8 易验证知 $(\varsigma, \xi_T, \xi_R, \chi; f, g)$ 是一个 $A^2$–码，利用文献 [4] 的引理 2 和引理 3，可证得如下的

**定理 5** 构作 (3) 所得到的 $A^2$–码具有 $|\varsigma| = n_1 n_2 / n_3$, $|\xi_T| = q^{4(n-4)}$, $|\xi_R| = q^{2(n-4)}(q^2+1)$, $|\chi| = |\varsigma||\xi_T|/n_4$；其中 $n_1 = N(2r-1, 2r-2; n-4)$, $n_2 = N(m_0 - 2r - 1, r_0 - 2r + 2; n - 2r - 4) + (q^{2(m_0-2r+1)} - 1) \times N(m_0 - 2r - 2, r_0 - 2r; n - 2r - 4)$, $n_3 = N(m_0 - 2, r_0; n-4)$, $n_4 = q^{4(2r-1)}$。

**定理 6**　构作 (3) 所得到的 $A^2$-码中，若发方的编码规则和收方的译码规则都按等概率分布选取，则各种攻击成功的概率分别为 $P_I = 1/q^{2(n-2r-3)}$, $P_S = 1/q^2$, $P_T = 1/(q^2+1)$, $P_{R_0} = 1/q^{2(n-2r-3)}$, $P_{R_1} = 1/q^2$

## 6 结束语

自 1992 年文献 [5] 发表以来，人们用有限域上酉几何先后构作出 10 类 Cartesian 认证码 ( $A$-码)；详细情况请参见文献 [4-7, 9, 10]，这些认证码无论参数和成功的攻击概率都不相同，并且其中还得到 5 组最优或近优的 $A$-码。与 $A$-码构造所取得的结果相比较，文献 [2, 3] 及本文只构造出五类 $A^2$-码，可见用酉几何构作 $A^2$-码还有待进一步深入探讨的必要。能否用酉几何构作出几类文献 [11] 所定义的完备的 (perfect) $A^2$-码，值得更好的研究。

## 参 考 文 献


[1] G. J. Simmons, Message authentication with arbitration of transmitter/reciver disputes, In: D. Chaum, W. L. Prica, eds., Proc. Eurocrypt'87, Amsterdan, Netherlands, 1987, April, 13–15, Springer Verlag Berlin, 1988, 151–165.

[2] Li Ruihu, Guo Luobin, Construction of authentication codes with arbitration from unitary geometry, Appl. Math.-JCU Ser. B., 1999, 14(4), 475–480.

[3] 马文平，王新梅，基于酉几何的具有仲裁的认证码的构造，应用数学学报，2000, 23(2), 289–293.

[4] 李瑞虎，赵全习，郭罗斌，利用酉几何构作新的 Cartesian 认证码 (II)，通信保密，2000(1)，总第 81 期，43–49.

[5] Wan Zhexian, Construction of Cartesian authentication codes from unitary geometry, Designs, Codes and Cryptography, 1992, 2, 336–356.

[6] Gao Suogang, Two construction of Cartesian authentication codes from unitary geometry, Appl. Math-JCU. Ser. A., 1996, 11(3), 343–354.

[7] Fen Rongquan, Wan Zhexian, A construction of Cartesian authentication codes from geometry of classical groups, J. Combinatories, Information and System Science, 1995, 20(3), 197–210.

[8] Wan Zhexian, Geometry of Classical Groups over Finite Fields, Student Litterature, Lund, 1993.

[9] Fen Rongquan, Another construction of Cartesian authentication codes from geometry of classical groups, Northeast. Math. J., 1999, 15(1), 103–114.

[10] 李瑞虎，郭罗斌，赵全习，利用酉几何构作新的 Cartesian 认证码，通信保密，1999(4)，总第 80 期，44–47.

[11] T. Johansson, Low bounds on the probability of deception in authentication with arbitration, IEEE Trans. on Info. Theory, 1994, IT-40(5), 1573–1585.


# FUTHER CONSTRUCTION OF AUTHENTICATION CODES WITH ARBITRATION RFOM UNITARY GEOMETRY


Li Ruihu* **　　Li Zhihui*　　Li Xueliang*

*(*Department of Appl. Math., Northwestern Polytechnical University, Xi'an* 710072, *China*)

**(*Missile Institute of Air Force Engineering University, Sanyuan* 713800, *China*)



**Abstract**　Three families of authentication codes with arbitration are constructed from unitary geometry, the parameters of the codes are computed. Assuming the encoding rules of the transmitter and the decoding rules of the receiver are chosen according to a uniform probability distribution, the probabilities of each kind of deceptions are also computed.



**Key words**　Finite fields, Unitary geometry, Authentication codes, Arbiter



李瑞虎：　男，1966 年生，副教授，目前从事代数编码与密码，代数学的教学与研究。

李志慧：　女，1966 年生，博士生，目前从事密码学、代数学方面的教学与研究工作。

李学良：　男，1958 年生，教授，目前从事图论，代数学与密码方面的教学与研究。