西安电子科技大学学报 2007 34 (3): 505-508 ISSN: 1001-2400 CN: 61-1076/TN

两类Cartesian认证码的构造

刘金龙, 许宗泽

(南京航空航天大学 信息科学与技术学院，江苏 南京 210016)

收稿日期 修回日期 网络版发布日期 2007-5-31 接受日期

摘要 利用循环排法构造了一类最优Cartesian认证码，避免了其他构造法所借助的群(或域)上的复杂运算. 对于任意两个相互无关的参数k，n，采用迭代法构造了一类信源数为k，且使敌方模仿攻击和替换攻击成功的概率均为1/n的Cartesian认证码;在相同参数k，n的条件下，与已知的笛卡尔积构造法相比，利用迭代法所构造的Cartesian认证码的编码规则数目减少了.

关键词 Cartesian认证码 最优Cartesian认证码 正交排列

分类号 TN918

Construction of two sorts of cartesian authentication codes

LIU Jin-long,XU Zong-ze

(Dept. of Info. Sci. and Tech., Nanjing Univ. of Aeronaut. and Astronaut, Nanjing 210016， China)

Abstract

A method to construct one sort of optimal Cartesian authentication codes by using the cyclic array is presented. The method is easy to realize and it needs no complicated calculation over group or finite fields. Another iterative means to construct one class of Cartesian authentication codes with the k sources and 1/n probabilities of successful impersonation and substitution attack is also proposed, where parameters k and n are two arbitrary positive integers. Compared with the Cartesian authentication codes constructed by Descartes product, the authentication codes produced by iterative means have far fewer encoding rules, when they contain the same parameters k and n.

Key words Cartesian authentication codes the optimal Cartesian authentication codes orthogonal arrays

DOI:

通讯作者