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

ZHANG Xiao-han¹, WANG Wen-xian²

(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


1) \( M_1 \) \( M_2 \) \( E_\mathcal{E} \) \( q^{k-2} \frac{q-1}{q-1} = q^{k-2}(q + 1) \)

2) \( \mathcal{E}_\mathcal{E} \) \( \mathcal{E}_\mathcal{E} \) \( \mathcal{E}_\mathcal{E} \) \( \mathcal{E}_\mathcal{E} \) \( \mathcal{E}_\mathcal{E} \) \( q^{k-2} \)

\[ \dim(M_1, M_2) = \dim(S_1, S_2) + \dim(E_T) - \dim(S_1, S_2, E_T) = k + 4 - 2k + 2 \]

\[ E_\mathcal{E} = U, \dim(M_1, M_2, P_0) = \dim(S_1, S_2) = k, \mathcal{E}_\mathcal{E} = 3 \]

3) \( A^2 = A^2, 0, 0 \) \( A^2 = A^2, 0, 0 \) \( A^2 = A^2, 0, 0 \)

\[ P_I = \frac{q^{k-2}}{(q^{k-2} - 1)} \]

\[ P_S = \frac{1}{q}, P_T = \frac{q^{-1}}{q^2 - 1} \]

\[ P_R = \frac{q^{k-2}}{(q^{k-2} - 1)} \]

\[ P_P = \frac{1}{q} \]

4) \( q^{k-2} \) \( \mathcal{E}_\mathcal{E} \) \( \mathcal{E}_\mathcal{E} \) \( \mathcal{E}_\mathcal{E} \) \( \mathcal{E}_\mathcal{E} \)

\[ d = q^{k-2}(q + 1), P_r = \frac{q^{k-2}}{q^{k-2} - 1} \]

\[ P_r = \max_k \frac{q^{k-2}}{q^{k-2} - 1} \]


