distance d is equivalent to the existence of certain sets of points called $(n, d-1)$-sets in the finite projective space $\mathbf{P}(\{0,1\}^r)$. For the sake of completeness, a set of n points in a projective space is an (n, s)-*set* if s is the largest integer such that every subset of s points is projectively independent. For example, an $(n, 3)$-set is a set of n points no three of which are collinear, but at least four of them are coplanar.

Other applications of projective geometry to cryptography are given in Chapter 6 of Beutelspacher and Rosenbaum [22].