On mutually unbiased Hadamard matrices and their applications in quantum cryptography

Hadi Kharaghani

University of Lethbridge

Canada

Abstract

A Hadamard matrix is a square matrix with ± 1-entries and orthogonal rows. Two Hadamard matrices H, K of order $4n^2$ are called *unbiased* if $HK^t = 2nL$, where L is a Hadamard matrix. Unbiased Hadamard matrices have applications in Association Schemes and Cryptography. It is conjectured that for each odd integer n there is a pair of unbiased Hadamard matrices of order $4n^2$. The situation for even values of n is quite different and quite interesting: The number of mutually unbiased Hadamard (=MUH) matrices of order $16n^2$ can not exceed $8n^2$. Not much is known about the largest number of MUH matrices of order $16n^2$ in general. A survey of what is known about MUH matrices and some applications will be discussed.