Bouyuklieva, Stefka; Varbanov, Zlatko
Some connections between self-dual codes, combinatorial designs and secret sharing schemes. (English) Zbl 1247.94045

Let $C = C^\perp$ be a binary self-dual code. It is doubly-even if each vector is of weight divisible by 4. If $C$ is not doubly-even then it is called singly-even. Let $C_0$ be the doubly-even subcode of a singly-even $C$, then $C_0^\perp \setminus C$ is called the shadow of $C$. The authors establish that the singly-even binary self-dual codes with parameters $[24m + 2, 12m + 1, 4m + 2]$ and $[24m + 18, 12m + 9, 4m + 4]$ having a shadow of minimum weight 1 have uniquely determined weight enumerators. From some of these codes the authors make use of the Assmus-Mattson theorem to produce 2- and 1-designs. Using these, they describe one-part and two-part secret-sharing schemes.

Reviewer: Chester J. Salwach (Easton)

MSC:

94B05 Linear codes (general theory)  
94A62 Authentication, digital signatures and secret sharing  
05B05 Combinatorial aspects of block designs

Keywords:

self-dual codes; secret-sharing schemes; combinatorial designs

Full Text: DOI