Pieprzyk, Josef; Zhang, Xian-Mo

**Ideal threshold schemes from MDS codes.** (English) [Zbl 1031.94538]


Summary: We observe that MDS codes have interesting properties that can be used to construct ideal threshold schemes. These schemes permit the combiner to detect cheating, identify cheaters and recover the correct secret. The construction is later generalised so that the resulting secret sharing is resistant against Tompa-Woll cheating [M. Tompa and H. Woll, J. Cryptology 1, 133-138 (1988; Zbl 0659.94008)].

For the entire collection see [Zbl 1015.00034].

**MSC:**

- 94A62 Authentication, digital signatures and secret sharing
- 94B05 Linear codes (general theory)  

**Keywords:**

- secret sharing
- threshold schemes
- cheating detection
- identification

**Full Text:** [Link](#)