MDS Codes, NMDS Codes and their Secret-Sharing Schemes

Dimitris E. Simos*
INRIA Paris-Rocquencourt
Project-Team SECRET
78153 Le Chesnay Cedex, France
email: dimitrios.simos@inria.fr

Zlatko Varbanov
University of Veliko Tarnovo
Department of Information Technologies
2 T.Tarnovski Str, 5000, Bulgaria
email: zl.varbanov@uni-vt.bg

In this work, we consider some methods to generate secret-sharing schemes from MDS and near-MDS codes. MDS (and NMDS) codes exhibit close connections with secret-sharing schemes. These connections and respective construction methods are given in [5], [7]. We combine these methods with some recent results on MDS and NMDS codes ([4]), and in the aftermath we are able to construct secret-sharing schemes for new parameters.

Let $F_q = GF(q)$ be a Galois field and F_q^n be an n-dimensional vector space over F_q. A linear code of length n and rank k is a linear subspace C with dimension k of the vector space F_q^n (also denoted $[n, k]_q$ for short). Such a code will be called a q-ary code. The number of nonzero coordinates of a given vector $x \in F_q^n$ is called *(Hamming) weight* of the vector. An $[n, k, d]_q$ code is an $[n, k]_q$ code with minimum weight at least d among all nonzero codewords. An $[n, k, d]_q$ code is called *maximum distance separable (MDS)* if $d = n - k + 1$. The Singleton defect of an $[n, k, d]_q$ code C defined as $s(C) = n - k + 1 - d$ measures how far C is away from being MDS. A code C with Singleton defect $s(C) = 1$, that is a $[n, k, n - k]_q$ code is called *almost MDS* (AMDS for short) [2]. An $[n, k, n-k]_q$ AMDS code for which the dual code is also an AMDS code, that is $s(C) = s(C^\perp) = 1$ is called a near-MDS code (NMDS for short) [3].

A **secret-sharing scheme** is a way of sharing a secret among a finite set of people or entities such that only some distinguished subsets of these have access to the secret. The collection Γ of all such distinguished subsets is called the **access structure** of the scheme. A *perfect* secret-sharing scheme for Γ is a method by which the shares are distributed to the parties such that:

(1) any subset in Γ can reconstruct the secret from its shares, and

(2) any subset not in Γ can never reveal any partial information on the secret (in the information theoretic sense).

In particular, secret sharing is said to be *ideal* if it is perfect and the size of the shares is equal to the size of the secrets. Secret-sharing schemes were first introduced by Blakley [1] and

*This work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme. This Programme is supported by the Marie Curie Co-funding of Regional, National and International Programmes (COFUND) of the European Commission.

Shamir [6] for the threshold case, that is, for the case where the subsets that can reconstruct the secret are all the sets whose cardinality is at least a certain threshold.

Construction 1 (Pieprzyk and Zhang [5]) *Let G be a generator matrix of an $[n+1, k, n-k+2]_q$ MDS code. Thus G is a $k \times (n+1)$ matrix over F_q. Set*

$$(s_0, s_1, \ldots, s_n) = (r_1, \ldots, r_k)G \tag{1}$$

where each $r_j \in F_q$. For any fixed $r_1, \ldots, r_k \in F_q$, $s_0, s_1, \ldots, s_n$ can be calculated from (1). These $s_1, \ldots, s_n$ are the shares for participants $P_1, \ldots, P_n$ respectively, and s_0 is the secret corresponding to the shares $s_1, \ldots, s_n$.

This scheme is ideal (was proved in [5]), however the number of participants n can be at most q, and therefore is limited by the size of the field. Moreover, in the scheme proposed in [7] (also an ideal scheme, this time based on NMDS codes), this bound on the number of the participants was improved to $q + 2\sqrt{q}$.
Considering these properties, MDS and NMDS codes over large fields have to be searched in order to construct secret-sharing schemes having the maximum number of participants. For example, over F_{197} there exist [10,5,6] MDS and [8,4,4] NMDS self-dual codes [4]. These codes were derived from combinatorial constructions based on computational searches of solutions of diophantine equations. Applying these parameters, secret-sharing schemes with 9 and 7 participants can be generated (for the MDS and near-MDS code, respectively). For this field the the maximum possible number of participants is 197 (for MDS codes) and 225 (for NMDS codes).

References

[1] G.R. Blakley, Safeguarding cryptographic keys. In Proc. of the 1979 AFIPS National Computer Conference, 313–317 (1979)

[2] M.A. de Boer, Almost MDS codes, *Des. Codes Cryptogr.*, **9** (1996), 143–155.

[3] S. Dodunekov and I.N. Landjev, On near-MDS codes, *J. Geom.* **54** (1995), 30–43.

[4] I.S. Kotsireas, C. Koukouvinos and D.E. Simos, MDS and near-MDS self-dual codes over large prime fields, *Adv. Math. Commun.*, **3** (2009), 349–361.

[5] J. Pieprzyk and X.-M. Zhang, Ideal Threshold Schemes from MDS Codes, ICISC'02 Proceedings of the 5th international conference on Information security and cryptology, Lecture Notes in Computer Science, 2587, Springer Berlin/Heidelberg, 253–263 (2003)

[6] A. Shamir, How to share a secret, *Commun. ACM*, **22** (1979), 612–613.

[7] Y. Zhou, F. Wang, Y. Xin, S. Luo, S. Qing and Y. Yang, A secret sharing scheme based on near-MDS codes, Proceedings of IC-NIDC2009, 833–836 (2009)