FRAMEPROOF RANK DISTANCE CODES FOR COPYRIGHT PROTECTION OF DIGITAL DATA

W.B. Vasantha Kandasamy and R.S. Selvaraj

In this paper, we introduce frameproof Rank Distance (fpRD) codes for digital fingerprinting which is a recent topic of cryptographic interest. Current copyright laws are perhaps inadequate for dealing with digital data, leading to interest in developing other copyright production mechanisms, including digital watermarking techniques. A watermark is a signal added to digital data (audio, video or still images) that can be detected or extracted later to make an assertion about the data. This signal can serve various purpose viz., fingerprinting, ownership assertion, authentication and integrity verification, content protection, content labeling, using control and so on. An offending user-pirate may try different types of attacks to remove the watermark, in order to distribute illegal copies anonymously. Stronger attack results when several pirates collude and compare their independently marked copies so that they can detect and locate the differences and combine their copies into a new one whose watermark differs from all the pirate's.
Boneh and shaw introduced frameproof codes in 1995, as a method of “digital fingerprinting” which prevents a coalition of specified size $t$ from framing a user not in a coalition. To the best of our knowledge most of the work previously done on frameproof codes is about binary codes and codes over $\mathbb{GF}(p)$ ($p$ being prime) with Hamming metric. We in this paper, for the first time introduce the frameproof codes over the Galois field $\mathbb{GF}(q^n)$, $N > 1$, $q$ a prime or a prime power, with a rank metric, namely $fpRD$ codes. The essential requirement for a code to be frameproof are fulfilled by the since a RD code has a RD code has a capability to hold large number of codewords in it. Moreover, it also has the metric (rank metric), which takes care of any linear or complex relationship the symbols of the alphabet could have among one another.

In the sequel, we introduce the concept of interesting RD codes and discuss them. We also define $t$-flameproof RD codes ($t > 2$) and give the existence of such codes. By this, no coalition of at most $t$ users can frame a user who is not in the coalition. Our study with $t$-ford codes opens up the floodgates of so many remarkable applications to copyright protection of digital data.