MSc project idea: **Watermarking codes**

It is possible to embed hidden data in digital content such as audio and video. This is called *watermarking* or *fingerprinting*. In *forensic watermarking* a content provider embeds a unique identification code into the content for each individual customer, in order to be able to trace any 'leakage' of content (e.g. distribution on P2P) back to the customer. The most powerful attack against forensic watermarks is the so-called *collusion attack*: multiple attackers collaborate to remove the watermark. As they have bought differently watermarked versions of the same content, they can find the location of a significant part of their watermarks simply by comparing their content. In these locations they have a strong attack. The content provider's defense is to use special error-correcting codewords as the embedded indentifiers.
This research topic involves information theory, statistics and analysis. See the webpage of the CREST project.

Possible research topics are

- numerical studies of score systems and attacks
- dynamic fingerprinting
- the link between fingerprinting, group testing and differential privacy
- alternative attacker models
- advanced statistics

Please contact dr. Boris Škorić if you are interested
MF 6.059
040-247 4870
b.skoric@tue.nl