Cryptology ePrint Archive: Report 2013/154

Optimal Suspicion Functions for Tardos Traitor Tracing Schemes

Jan-Jaap Oosterwijk and Boris Skoric and Jeroen Doumen

Abstract: We investigate alternative suspicion functions for Tardos traitor tracing schemes. In the simple decoder approach (computation of a score for every user independently) we derive suspicion functions that optimize a performance indicator related to the sufficient code length ℓ in the limit of large coalition size c. Our results hold for the Restricted-Digit Model as well as the Combined-Digit Model. The scores depend on information that is usually not available to the tracer -- the attack strategy or the tallies of the symbols received by the colluders. We discuss how such results can be used in realistic contexts.

We study several combinations of coalition attack strategy vs. suspicion function optimized against some attack (another attack or the same). In many of these combinations the usual scaling $\ell \propto c^2$ is replaced by a lower power of c, e.g. $c^{3/2}$. We find that the interleaving strategy is an especially powerful attack, and the suspicion function tailored against interleaving is effective against all considered attacks.

Category / Keywords: Traitor tracing

Publication Info: Submitted to IHMMSEC 2013

Date: received 14 Mar 2013, last revised 14 Mar 2013

Contact author: J Oosterwijk at tue nl