THAÍS IDALINO, Universidade Federal de Santa Catarina
Modification-Tolerant Signature Schemes

Classical digital signature schemes are used to guarantee that a document was created by the sender (authenticity) and has not been modified along the way (integrity). However, the signature verification algorithm has a boolean output: a successful outcome is achieved if and only if both the signature is valid and the document has not been modified.

In this work, we consider more general digital signature schemes which we call modification-tolerant signature schemes, which go beyond the ability of detecting modifications, and have the ability of locating modifications or locating and correcting modifications. They can be used in applications where either the data can be modified (collaborative work), or the data must be modified (redactable and content extraction signatures) or we need to know which parts of the data have been modified (data forensics).

We discuss two types of modification-tolerant signature schemes: a general one that allows the location of modified blocks of the data, and a scheme with correction capability, that allows the correction of the modified blocks, recovering the original message. We give three instantiations of the scheme for the purpose of location, correction, and redaction. The schemes are proposed using techniques from combinatorial group testing.

This talk is based on joint work with Lucia Moura and Carlisle Adams.