Tamper Detection and Non-malleable codes

Daniel Wichs, Northeastern University

In this talk, we consider a setting where a codeword can be adversarially tampered via a function from some family of "tampering functions". We discuss the different types of security guarantees that can be achieved in this setting for various tampering families. We begin with tamper-detection codes, which must detect that tampering occurred. We then move on to a natural relaxation of tamper-detection, called non-malleable codes, which require that a tampered codeword either decodes to the original message m, or to some unrelated value that doesn't provide any information about m. We focus on existential results and understanding which function families admit such codes, but will also discuss some examples of explicit constructions.