1106-68-1575 **Mahdi Cheraghchi*** (mahdi@csail.mit.edu), MIT CSAIL, 32 Vassar Street, Cambridge, MA 02139. *Capacity and Constructions of Non-Malleable Codes.*

Non-malleable codes, introduced by Dziembowski, Pietrzak and Wichs (ICS 2010) and motivated by applications in tamper-resilient cryptography, encode messages in a manner so that tampering the codeword causes the decoder to either output the correct message or an uncorrelated message. While this relaxation of error detection is an impossible goal to achieve against unrestricted tampering functions, rather surprisingly non-malleable coding becomes possible against any fixed family of tampering functions that is not too large. The following subjects will be discussed:

1. "Capacity" of non-malleable codes: For any tampering family of a prescribed size, an optimal bound is derived on the maximum possible rate of a non-malleable code against the given family.

2. An efficient Monte-Carlo construction of non-malleable codes against any family of tampering functions of exponential size (e.g., polynomial-sized Boolean circuits) is given.

3. The specific family of bit-tampering adversaries, that is adversaries that independently act on each encoded bit, will be considered. For this family, an explicit construction of non-malleable codes achieving rate arbitrarily close to 1 is discussed.

Based on joint work with Venkatesan Guruswami and articles arXiv:1309.0458, arXiv:1309.1151. (Received September 14, 2014)