Pilshchikov, D. V.
On the limiting mean values in probabilistic models of time-memory-data tradeoff methods.
(Russian. English summary) [Zbl 1475.94048]

Summary: Time-memory-data tradeoff methods are used to solve one-way function inversion problems. This work provides some mathematical results aimed to the complexity analysis of the most known methods. We introduce a set of random variables depending on the generation sizes and on the total number of particles in a Galton-Watson process considered as a model of the main characteristics of these methods. The limit behavior of their mean values is studied. This work develops the results presented by the author at the CTCrypt 2013 workshop.

MSC:
94A17 Measures of information, entropy
94A60 Cryptography
60J80 Branching processes (Galton-Watson, birth-and-death, etc.)

Keywords:
time-memory-data tradeoff; one-way function inversion

Full Text: DOI MNR

References:

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.