Cryptology ePrint Archive: Report 2011/387

Analysis of the Parallel Distinguished Point Tradeoff

Jin Hong and Ga Won Lee and Daegun Ma

Abstract: Cryptanalytic time memory tradeoff algorithms are tools for quickly inverting one-way functions and many consider the rainbow table method to be the most efficient tradeoff algorithm. However, it was recently announced, mostly based on experiments, that the parallelization of the perfect distinguished point tradeoff algorithm brings about an algorithm that is 50\% more efficient than the perfect rainbow table method. Motivated by this claim, while noting that the massive pre-computation associated with any tradeoff algorithm makes the non-perfect forms of tradeoff algorithms more practical, we provide an accurate theoretic analysis of the parallel version of the non-perfect distinguished point tradeoff algorithm.

Performance differences between different tradeoff algorithms are usually not very large, but even these small differences can be crucial in practice. So we take care not to ignore the side effects of false alarms in providing an online time complexity analysis of the parallel distinguished point tradeoff algorithm. Our complexity results are used to compare the parallel non-perfect distinguished point tradeoff against the non-perfect rainbow table method. The two algorithms are compared under identical success rate requirements and the pre-computation efforts are also taken into account. Contrary to our anticipation, we find that the rainbow table method is superior in typical situations, even though the parallelization did have a positive effect on the efficiency of the distinguished point tradeoff algorithm.

Category / Keywords: time memory tradeoff, parallel distinguished point, distinguished point, rainbow table

Date: received 18 Jul 2011, last revised 18 Jul 2011

Contact author: gwlee87 at snu ac kr