Pil'shchikov, D. V.

A complexity analysis of algorithm of parallel search of the "gold" collision. (Russian. English summary) Zbl 1472.68231

Mat. Vopr. Kriptografii 6, No. 4, 77-97 (2015).

Summary: The paper refines known estimates of time and memory complexities of Oorschot and Wiener algorithm for the "gold" collision searching. We use results related to the computation of characteristics of time-memory-data tradeoff method with distinguished points. Probabilistic approximations of the algorithm characteristics by random variables depending on the number of particles and the total number of particles in a subcritical Galton-Watson process are described. The limits of expectations of these random variables are found.

MSC:

68W40 Analysis of algorithms
94A60 Cryptography

Keywords:

gold collision search; time-memory-data tradeoff with distinguished points; branching processes; one-way function inversion

Full Text: DOI MNR

References:

[1] Oorschot P. C., Wiener M. J., "Parallel collision search with cryptanalytic applications", J. Cryptology, 12 (1999), 1-28 · Zbl 0992.94028 · doi:10.1007/PL00003816

[2] Oorschot P. C., Wiener M. J., "Parallel collision search with application to hash functions and discrete logarithms", 2nd ACM Conf. on Computer and Commun. Security, Fairfax, Virginia, 1994, 210-218

[3] Oorschot P. C., Wiener M. J., "Improving implementable meet-in-the-middle attacks by orders of magnitude", CRYPTO' 96, Lect. Notes Comput. Sci., 1109, 1996, 229-236 · Zbl 1329.94083 · doi:10.1007/3-540-68697-5$_1$8

[4] Borst J., Preneel B., Vandewalle J., "On the time-memory tradeoff between exhaustive key search and table precomputation", Proc. 19th Symp. Inf. Theory in the Benelux, Veldhoven, Netherlands, 1998, 111-118

[5] Standaert F. X., Rouvroy G., Quisquater J. J., Legat J. D., "A time-memory tradeoff using distinguished points: New analysis \& FPGA results", Proc. CHES 2002, Lect. Notes Comput. Sci., 2523, 2003, 596-611 · Zbl 1020.94526

[6] Pilshchikov D. V., "Estimation of the characteristics of time-memory-data tradeoff methods via generating functions of the number of particles and the total number of particles in the Galton-Watson process", Matematicheskie voprosy kriptografii, 5:2 (2014), 103-108 · Zbl 1475.60168

[7] Pilshchikov D. V., "On the limiting mean values in probabilistic models of time-memory-data tradeoff methods", Matematicheskie voprosy kriptografii, 6:2 (2015), 59-65 · Zbl 1475.94048