Pilshchikov, D. V.

On the limiting mean values in probabilistic models of time-memory-data tradeoff methods.
(Russian. English summary) Zbl 1475.94048
Mat. Vopr. Kriptografii 6, No. 2, 59-65 (2015).

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:

[1] Vatutin V. A., Sagitov S. M., "A decomposable critical branching process with two types of particles", Trudy Matem. in-ta im. V. A. Steklova, 177, 1986, 3-20 (in Russian) · Zbl 0619.60079

[2] Aliev S. A., Shurenkov V. M., "Transitional phenomena and the convergence of Galton-Watson processes to Jirina processes", Teoriya veroyatn. i ee primen., 27:3 (1982), 443-455 (in Russian) · Zbl 0565.60068

[3] Avoine G., Junod P., Oechslin P., Time-memory trade-offs: False alarm detection using checkpoints (extended version), Tech. Rept LASEC-REPORT 2005-002, 2005 · Zbl 1153.94345

[4] Avoine G., Junod P., Oechslin P., "Characterization and improvement of timememory trade-off based on perfect tables", ACM Trans. Inf. and Syst. Secur., 11:4 (2008), Article 17, 22 pp. · Zbl 1138.68338 · doi:10.1145/1380564.1380565

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

[6] Matsumoto T., Kim I., Hara T., "Methods to reduce time and memory in timememory tradeoff", ISEC, 1997, 97-100

[7] Hellman M. E., "A cryptanalytic time-memory trade off", IEEE Trans. Inf. Theory, IT-26:4 (1980), 401-406 · Zbl 0436.94016 · doi:10.1109/TIT.1980.1056220

[8] Hong J., "The cost of false alarms in Hellman and rainbow tradeoffs", Des. Codes and Cryptogr., 57:3 (2010), 293-327 · Zbl 1197.94192 · doi:10.1007/s10623-010-9368-x

[9] Hong J., Jeong K. C., Kwon E. Y., Lee I.-S., Ma D., "Variants of the distinguished point method for cryptanalytic time memory trade-off", ISPEC 2008, Lect. Notes Comput. Sci., 4991, Springer-Verlag, 2008, 131-145

[10] Kim I.-J., Matsumoto T., "Achieving higher success probability in time-memory trade-off cryptanalysis without increasing memory size", IEICE Trans. Fundam. Electr., Communic. Comput. Sci., E82-A:1 (1999), 123-129

[11] Ma D., Hong J., "Success probability of the Hellman trade-off", Inf. Process. Lett., 109:7 (2009), 347-351 · Zbl 1191.68282 · doi:10.1016/j.ipl.2008.12.002

[12] Oechslin P., "Making a faster cryptanalytic time-memory trade-off", CRYPTO'03, Lect. Notes Comput. Sci., 2729, 2003, 617-630 · Zbl 1122.94393

[13] 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, 2002, 593-609 · Zbl 1020.94526

[14] Pakes A. G., "Some limit theorems for the total progeny of a branching process", Adv. Appl. Probab., 3:1 (1971), 176-192 · Zbl 0218.60075 · doi:10.2307/1426333

[15] Hoch Y.Ż., Security analysis of generic iterated hash functions, Ph. D. Thesis, Weizmann Inst. of Sci., Rehovot, 2009

[16] Hong J., Moon S., "A comparison of cryptanalytic tradeoff algorithms", J. Cryptology, 26:4 (2013), 559-637 · Zbl 1283.94069 · doi:10.1007/s00145-012-9128-3

[17] Lee G. W., Hong J., A comparison of perfect table cryptanalytic tradeoff algorithms, Cryptology ePrint Archive, Report 2012/540 · Zbl 1402.94061

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