МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 1 С. 95–106

УДК 519.719.2+519.712

Асимптотическое поведение мощности полного прообраза образа случайного множества при итерациях отображений конечного множества

Д. В. Пильщиков

Лаборатории ТВП, Москва

Получено 30.V.2016

Аннотация. В связи с оценками сложности алгоритмов балансировки времени-памяти-данных возникают задачи оценки мощности полного прообраза образа случайного множества при многократных итерациях отображений. Предложена вероятностная модель, описывающая мощности исследуемых случайных множеств величинами, зависящими от числа частиц и суммарного числа частиц в процессе Гальтона – Ватсона. Найдены пределы математических ожиданий этих случайных величин.

Ключевые слова: образ случайного множества, мощность прообраза, метод Хеллмана, балансировка времени-памяти с особыми точками

Asymptotic behaviour of the complete preimage cardinality for the image of a random set under iterations of mappings of a finite set

D. V. Pilshchikov

TVP Laboratories, Moscow

Abstract. The estimation of complexity of time-memory-data tradeoff algorithms leads to the estimation problems of the complete preimage cardinality for the image of a random set under multiple iterations of mappings. We describe a probabilistic model allowing to estimate the cardinalities of the random sets considered via the number of particles and the total number of particles in the Galton – Watson process. The limits of mean values of these random variables are found.

Key words: image of a random set, preimage cardinality, Hellman method, time-memory tradeoff with distiguished points

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 95–106 (Russian)

Список литературы

[1] Avoine G., Junod P., Oechslin P., “Characterization and improvement of time-memory trade-off based on perfect tables”, *Trans. Inf. Syst. Secur.*, **11**:17 (July 2008), 1–17.

[2] Borst J., Preneel B., Vandewalle J., “On the time-memory tradeoff between exhaustive key search and table precomputation”, *Symp. Inf. Theory in the Benelux* (1998), 111–118.

[3] Hellman M. E., “A cryptanalytic time-memory trade off”, *IEEE Trans. Inf. Theory*, **IT-26** (1980), 401–406.

[4] Hong J., “The cost of false alarms in Hellman and rainbow tradeoffs”, *Des., Codes and Cryptogr.*, **57**:3 (2010), 293–327.

[5] Oechslin P., “Making a faster cryptanalytic time-memory trade-off”, CRYPTO’03, Lect. Notes Comput. Sci., **2729**, 2003, 617–630.

[6] Standaert F. X., Rouvroy G., Quisquater J. J., Legat J. D., “A time-memory tradeoff using distinguished points: New analysis & FPGA results”, CHES 2002, Lect. Notes Comput. Sci., **2523**, 2002, 593–609.

[7] Hoch Y. Z., *Security analysis of generic iterated hash functions*, Ph.D. Thesis, Weizmann Inst. of Sci., 2009.

[8] Hong J., Moon S., “A comparison of cryptanalytic tradeoff algorithms”, *J. Cryptology*, **26** (2013), 559–637.

[9] Pilshchikov D. V., “On the limiting mean values in probabilistic models of time-memory-data tradeoff methods”, *Mathematical Aspects of Cryptography*, **6**:2 (2015), 59–65.

[10] Севастьянов Б. А., *Ветвящиеся процессы*, М.: Наука, 1971.