D. V. Pilshchikov, О предельных средних значениях в вероятностных моделях методов балансировки времени-памяти-данных, *Матем. вопр. криптогр.*, 2015, том 6, выпуск 2, 59–65

DOI: 10.4213/mvk145

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2015 Т. 6 № 2 С. 59–65

УДК: 519.719.2+519.712.4

On the limiting mean values in probabilistic models of time-memory-data tradeoff methods

D. V. Pilshchikov

TVP Laboratory, Moscow

Получено 16.IX.2014

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.

Key words: time-memory-data tradeoff, one-way function inversion

О предельных средних значениях в вероятностных моделях методов балансировки времени-памяти-данных

Д. В. Пильщиков

Лаборатория ТВП, Москва

Аннотация. Методы балансировки времени-памяти-данных используются при решении задачи обращения однонаправленных функций. Статья содержит математические результаты, предназначенные для анализа сложности большинства известных методов. Вводится множество случайных величин, зависящих от размеров поколений и от общего числа частиц в процессе Гальтона–Ватсона, рассматриваемого как модель основных характеристик этих методов. Изучается предельное поведение их средних значений. Работа продолжает исследования, представленные автором на мини-симпозиуме CTCrypt 2013.

Ключевые слова: балансировка времени-памяти-данных, обращение однонаправленных функций

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 2, pp. 59–65 (Russian).

In [3]–[13] a problem of inversion of one-way function was considered. This problem may be summarized as follows.

Let

$$G : X \to X$$

be a one-way function defined on a set X, $|X| = N$, and $\mathcal{D}$ be a set of D elements of set X of the form

$$\mathcal{D} = \{y_i \in X | y_i = G(x_i),\ i \in \overline{1, D}\},$$

where set

$$\bar{\mathcal{D}} = \{x_i \in X,\ i \in \overline{1, D}\}$$

is unknown. The goal is to find at least one element of the set $\bar{\mathcal{D}}$ given the set $\mathcal{D}$.

Time-memory-data tradeoff methods are widely used to solve this problem. The most popular are the following three methods:

- Hellman method (HM-method) [7],
- distinguished points method (DP-method) [5, 13],
- rainbow tables method (RM-method) [12].

Any time-memory-data tradeoff method consists of two phases: pre-computation phase and online phase, in each case chains of some F-operations are calculated. Each such chain is a sequential evaluation of the function (F-operation) of the form

$$F(x) = R(G(x)), x \in X,$$

where $R : X \to X$ is a bijective function.

At the pre-computation phase the tables consisting of starting and ending points of calculated chains are constructed.

A solution of the problem of one-way function inversion is found at the online phase using the tables constructed. During the online phase, two types of chains are constructed: basic and additional. Basic chains start from elements of the set $\mathcal{D}$. If the end of the basic chain belongs to the pre-computed table, then an additional chain of F-operations is being calculated and among the elements of this chain the solution is searched.

In order to increase the efficiency of HM-, DP- and RM-methods in [4, 13, 15] their modifications were suggested. In [4] DP- and RM-methods with perfect tables (DPP- and RMP-methods) were described. In [13] the possibility to bound the chain length in DP- and DPP-methods was shown, as well as the possibility to

bound the chain length information stored in the table. In [15] OCR-technique for constructing additional chains (DP-OCR- and DPP-OCR-methods) was suggested.

The main parameters of these methods are: the size of the set X, the length of chains, the size and the number of tables used. The main characteristics of these methods are: the probability of success, the (mean) number of F-operations performed at the pre-computation and online phases (including construction of basic and additional chains), the number of additional chains and the number of table lookups. The most comprehensive overview of results on the relationship between parameters and characteristics of these methods may be found in [16, 17].

In the paper [18] we suggest a probabilistic model allowing to apply the results of [16, 17] to the case when the function G has specific properties (namely, the value $B = \frac{1}{N}\left(\sum_{x\in X}\left|G^{-1}(x)\right|^2\right) - 1$ is not close to 1), and to estimate all main characteristics for all modifications considered. In this model the characteristics of time-memory-data tradeoff methods are described by the mean values of random variables depending on the number of particles $\mu(i)$ in the i-th generation of critical or subcritical Galton-Watson process $\mu(t), t = 0, 1, \ldots$, and on the total number of particles $v(j,k) = \sum_{l=j}^{k-1}\mu(l)$. Namely, these mean values are:

$$\mathbf{E}\mu(j)\cdot\mu(k),\ \mathbf{E}v(j,k),\ \mathbf{E}\mu(i)\,v(j,k),\ \mathbf{E}u^{\mu(j)},$$

$$\mathbf{E}u^{\mu(j)},\ \mathbf{E}u^{v(j,k)},\ \mathbf{E}\mu(j)u^{\mu(j)-1},\ \mathbf{E}\mu(i)u^{v(j,k)},\ \mathbf{E}\mu(i)\cdot u^{\mu(j)},\ \mathbf{E}v(i)u^{v(j,k)},$$

$$\mathbf{E}\mu(i)u^{v(j-1,k)} - \mathbf{E}\mu(i)u^{v(j,k)},\ \mathbf{E}u^{v(j-1,k)} - \mathbf{E}u^{v(j,k)},$$

where i, j, k are natural numbers large enough and u is a real number close enough to 1.

The estimates of characteristics are obtained by means of the limits of mean values described above under some conditions on the growth of variables i, j, k, u. The limits are expressed in terms of the functions $f_{A,B}(x,y,z)$, $\tilde{f}_{A,B}(x,y,z)$ introduced in [18]:

$$f_{A,B}(x,y,z) = \frac{1}{B/2} f_1\left(x, y\cdot B/2 + A/2, z\cdot B/2 + \left(\frac{A}{2}\right)^2\right) - (A/B),$$

$$f_1(x,y,z) = \frac{1}{x} f_0\left(yx, zx^2\right), x > 0,\ f_1(0,y,z) = y,$$

$$f_0(y,z) = \frac{y + \sqrt{z}\cdot \operatorname{th}\left(\sqrt{z}\right)}{1 + y\cdot\frac{\operatorname{th}\sqrt{z}}{\sqrt{z}}}, z > 0,\ f_0(y,0) = \frac{y}{1+y},$$

$$\tilde{f}_{A,B}(x,y,z) = \frac{\partial f_{A,B}(x,y,z)}{\partial y}\,.$$

Now we describe the results on the limiting behavior of the mean values described above. Consider the sequences of natural numbers t_s, i_s, j_s, k_s, nonnegative real numbers y_s, z_s and Galton-Watson processes $\{\mu_s(i), i = 0, 1, \dots\}$, $s \in 1, 2, \dots$ Suppose that three first factorial moments of random variables $\mu_s(1)$, $s \in 1, 2, \dots$, are finite:

$$\mathbf{E}\mu_s(1) = 1 - \frac{A_s}{t_s},\ A_s \geq 0,$$

$$\mathbf{E}\mu_s^{(2)}(1) = B_s,\ B_s > 0,$$

$$\mathbf{E}\mu_s^{(3)}(1) = R_s.$$

Let the following asymptotic relationships AC as $s \to \infty$ be valid:

$$A_s \to A,\ B_s \to B > 0,$$

$$t_s \to \infty,\ \frac{i_s}{t_s} \to x_0,\ \frac{j_s}{t_s} \to x_1,\ \frac{k_s}{t_s} \to x_2,\ x_1 < x_2,$$

$$y_s \to y,\ z_s \to z,$$

and sequence $R_s, s \in 1, 2, \dots$, be bounded.

Theorem 1. *If the condition AC is satisfied, then as* $s \to \infty$

1) $\frac{1}{t_s}\mathbf{E}\mu_s(i_s) \cdot \mu_s(j_s) \to B\left(\frac{1-e^{-Ax_0}}{A}\right)e^{-Ax_1}$ *if* $A > 0$,

2) $\frac{1}{t_s}\mathbf{E}\mu_s(i_s) \cdot \mu_s(j_s) \to Bx_0$ *if* $A = 0$,

3) $\frac{1}{t_s}\mathbf{E}v_s(i_s, j_s) \to e^{-Ax_0}\left(\frac{1-e^{-A(x_1-x_0)}}{A}\right)$ *if* $A > 0$,

4) $\frac{1}{t_s}\mathbf{E}v_s(i_s, j_s) \to x_1 - x_0$ *if* $A = 0$,

5) $\frac{1}{t_s^2}\mathbf{E}\mu_s(i_s)\,v_s(j_s, k_s) \to B\left(\frac{1-e^{-Ax_0}}{A}\right)\left(\frac{e^{-Ax_1}-e^{-Ax_2}}{A}\right)$ *if* $x_0 < x_1 < x_2$ *and* $A > 0$,

6) $\frac{1}{t_s^2}\mathbf{E}\mu_s(i_s)\,v_s(j_s, k_s) \to Bx_0(x_2 - x_1)$ *if* $x_0 < x_1 < x_2$ *and* $A = 0$,

7) $\frac{1}{t_s^2}\mathbf{E}\mu_s(i_s)v_s(j_s, k_s) \to Be^{-Ax_0}\left(x_2 - x_1 - \left(e^{-Ax_1} - e^{-Ax_2}\right)A^{-1}\right)A^{-1}$ *if* $x_1 < x_2 < x_0$ *and* $A > 0$,

8) $\frac{1}{t_s^2}\mathbf{E}\mu_s(i_s)v_s(j_s, k_s) \to B(x_2 - x_1)(x_2 + x_1)/2$ *if* $x_1 < x_2 < x_0$ *and* $A = 0$,

9) $t_s\left(1-\mathbf{E}\left(1-\frac{y_s}{t_s}\right)^{\mu_s(i_s)}\right)\to f_{A,B}(x_0,y,0)$,

10) $t_s\left(1-\mathbf{E}\left(1-\frac{z_s}{t_s^2}\right)^{v_s(0,i_s)}\right)\to f_{A,B}(x_0,0,z)$,

11) $\mathbf{E}\mu_s(i_s)\left(1-\frac{y_s}{t_s}\right)^{\mu_s(i_s)-1}\to \tilde{f}_{A,B}(x_0,y,0)$.

Theorem 2. *If the condition AC is satisfied, then as* $s\to\infty$

1) $\mathbf{E}\mu_s(i_s)\left(1-\frac{z_s}{t_s^2}\right)^{v_s(j_s,k_s)}\to$

$$\tilde{f}_{A,B}\left(x_0,f_{A,B}\left(x_1-x_0,f_{A,B}\left(x_2-x_1,0,z\right),0\right),0\right),$$

if $x_0<x_1$,

2) $\mathbf{E}\mu_s(i_s)\left(1-\frac{z_s}{t_s^2}\right)^{v_s(j_s,k_s)}\to$

$$\tilde{f}_{A,B}\left(x_0-x_1,f_{A,B}\left(x_2-x_0,0,z\right),z\right)\cdot\tilde{f}_{A,B}\left(x_1,f_{A,B}\left(x_2-x_1,0,z\right),0\right),$$

if $x_1<x_0<x_2$,

3) $\mathbf{E}\mu_s(i_s)\left(1-\frac{z_s}{t_s^2}\right)^{v_s(j_s,k_s)}\to$

$$\tilde{f}_{A,B}\left(x_0-x_2,0,0\right)\cdot\tilde{f}_{A,B}\left(x_2-x_1,0,z\right)\cdot\tilde{f}_{A,B}\left(x_1,f_{A,B}\left(x_2-x_1,0,z\right),0\right),$$

if $x_2<x_0$,

4) $t_s\left(1-\mathbf{E}\left(1-\frac{z_s}{t_s^2}\right)^{v_s(j_s,k_s)}\right)\to f_{A,B}\left(x_1,f_{A,B}\left(x_2-x_1,0,z\right),0\right)$,

5) $\mathbf{E}\mu_s(i_s)\cdot\left(1-\frac{y_s}{t_s}\right)^{\mu_s(j_s)}\to\tilde{f}_{A,B}\left(x_0,f_{A,B}\left(x_1-x_0,y,0\right),0\right)$, *if* $x_0<x_1$.

Theorem 3. *If the condition AC is satisfied, then as* $s\to\infty$

1) $t_s\left(\mathbf{E}\mu_s\left(i_s\right)\left(1-\frac{z_s}{t_s^2}\right)^{v_s(j_s,k_s)}-\mathbf{E}\mu_s\left(i_s\right)\left(1-\frac{z_s}{t_s^2}\right)^{v_s(j_s-1,k_s)}\right)\to$

$$\frac{\partial\tilde{f}_{A,B}\left(x_0,f_{A,B}\left(x_1-x_0,f_{A,B}\left(x_2-x_1,0,z\right),0\right),0\right)}{\partial x_1},$$

if $x_0<x_1$,

2) $t_s\left(\mathbf{E}\mu_s\left(i_s\right)\left(1-\frac{z_s}{t_s^2}\right)^{v_s(j_s,k_s)}-E\mu_s\left(i_s\right)\left(1-\frac{z_s}{t_s^2}\right)^{v_s(j_s-1,k_s)}\right)\to$

$$\frac{\partial\tilde{f}_{A,B}\left(x_0-x_1,f_{A,B}\left(x_2-x_0,0,z\right),z\right)\cdot\tilde{f}_{A,B}\left(x_1,f_{A,B}\left(x_2-x_1,0,z\right),0\right)}{\partial x_1},$$

if $x_1\le x_0\le x_2$,

$$3)\ t_s^2\left(\mathbf{E}\left(1-\tfrac{z_s}{t_s^2}\right)^{v_s(j_s,k_s)}-E\left(1-\tfrac{z_s}{t_s^2}\right)^{v_s(j_s-1,k_s)}\right)\to$$

$$-\frac{\partial f_{A,B}\left(x_1, f_{A,B}\left(x_2-x_1,0,z\right),0\right)}{\partial x_1}.$$

References

[1] Vatutin V. A., Sagitov S. M., "A decomposable critical branching process with two types of particles", *Труды Матем. ин-та им. В. А. Стеклова*, **177** (1986), 3–20 (in Russian).

[2] Aliev S. A., Shurenkov V. M., "Transitional phenomena and the convergence of Galton–Watson processes to Jirina processes", *Теория вероятн. и ее примен.*, **27**:3 (1982), 443–455 (in Russian).

[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.

[4] Avoine G., Junod P., Oechslin P., "Characterization and improvement of time-memory trade-off based on perfect tables", *ACM Trans. Inf. & Syst. Secur.*, **11**:4 (2008), 22 pp.

[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 time-memory 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.

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

[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.

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

[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.

[14] Pakes A.G., "Some limit theorems for the total progeny of a branching process", *Adv. Appl. Probab.*, **3**:1 (1971), 176–192.

[15] Hoch Y. Z., *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.

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

[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", *Математические вопросы криптографии*, **5**:2 (2014), 103–108.