ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 21 **МАТЕМАТИКИ** **Выпуск 5**
2014

Д. В. Пильщиков (Москва, ТВП). **Об обосновании формулы надежности в методах балансировки время-память-данные.**

В докладе, представленном данным сообщением, предлагается теоретико-вероятностная модель, на основе которой выводится формула, задающая надежность метода Хеллмана и метода с особыми точками при обращении однонаправленной функции. Получены двухсторонние оценки надежности и вероятности решения задачи обращения однонаправленной функции при фиксированных таблицах. Данные оценки позволяют уточнить область применимости известных ранее формул для надежности алгоритмов обращения однонаправленных функций.

Рассмотрим задачу обращения однонаправленной функции. Ее можно сформулировать следующим образом.

Пусть имеется однонаправленная функция [1] $G : X \to X$, заданная на множестве $X, |X| = N$, и набор $\mathcal{D}$, состоящий из D элементов множества X вида $\mathcal{D} = \{y_i \in X | \, y_i = G(x_i), \ \ i = 1, 2, \ldots, D\}$, где $\{x_n \in X, \ n = 1, 2, \ldots, D\}$ есть некоторое неизвестное множество $\overline{\mathcal{D}}$. Требуется по множеству $\mathcal{D}$ найти хотя бы один элемент множества $\overline{\mathcal{D}}$.

Для решения задачи обращения однонаправленной функции широкое применение находят методы балансировки время-память-данные. Наибольшую известность из них получили три следующих метода:

— метод Хеллмана [2] (далее HM-метод),

— метод Хеллмана с особыми точками [3, 4] (далее DP-метод),

— метод Хеллмана с радужными таблицами [5].

Все методы балансировки время-память-данные состоят из двух этапов: предварительного и оперативного, в течение которых вычисляются цепочки F-операций. Каждая из цепочек представляет собой последовательное вычислений функций (F-операций) вида $F(x) = R(G(x)), \ \ x \in X$, где $R : X \to X$ — некоторое биективное отображение.

На предварительном этапе проводится построение и сохранение таблиц, в которых записываются начало и конец вычисленных цепочек. Решение задачи обращения однонаправленной функции происходит на оперативном этапе, при этом используются построенные таблицы.

В HM- и DP-методах (и их модификациях) на предварительном этапе строятся l таблиц T_i для l различных отображений $R_i, \ \ i = 1, 2, \ldots, l$. Обозначим M_i множество элементов, лежащих на цепочках F-операций, выполненных при построении таблицы $T_i, \ \ i = 1, 2, \ldots, l$. Задача обращения однонаправленной функции будет решена [3], если хотя бы один элемент множества $\overline{\mathcal{D}}$ лежит в объединении $\bigcup_{i=1}^{l} M_i$. Полагая, что элементы множества $\overline{\mathcal{D}}$ получены посредством равновероятной выборки с возвращением из X, легко получить следующую формулу для вероятности p

решения задачи обращения однонаправленной функции при фиксированных таблицах:

$$p = 1 - \left(1 - \frac{|\bigcup_{i=1}^{l} M_i|}{N}\right)^D.$$

Надежностью η метода балансировки время-память-данные естественно называть усредненное значение величины p. Усреднение рассматривается по всевозможным наборам функций R_i, $i = 1, 2, \ldots, l$, и всевозможным наборам начал цепочек в таблицах T_i, $i = 1, 2, \ldots, l$, в предположении равновероятности любого набора.

Заметим, что надежность η можно рассчитать путем усреднения по случайным множествам $M_1, M_2, \ldots, M_l$, на которых задана вероятностная мера, индуцированная описанным выше равновероятным распределением на множестве всевозможных наборов функций R_i, $i = 1, 2, \ldots, l$, и начал цепочек в таблицах T_i, $i = 1, 2, \ldots, l$. Данный подход и используется в предлагаемой далее вероятностной модели.

Пусть имеется набор из l случайных независимых подмножеств $M_1, M_2, \ldots, M_l$ множества $X, |X| = N$. Каждое из них имеет одинаковое распределение, которое определяется формулами

$$\mathbf{P}\{M_1 = M\} = \frac{p_{|M|}}{C_N^{|M|}},$$

где M — произвольное подмножество X. Через $f(z)$ обозначим производящую функцию $f(z) = \sum_{m=0}^{N} p_m z^m$ распределения мощности случайного подмножества $\{p_m,\ m = 0, 1, \ldots, N\}$, а через $f^{[k]}$ — ее k-й момент $f^{[k]} = \sum_{m=0}^{N} p_m m^k$.

Рассматривается случайная величина ξ, равная доле суммарного числа элементов множества X, находящихся хотя бы в одном из множеств $M_1, M_2, \ldots, M_l$. Данная величина выражается формулой

$$\xi = \frac{1}{N} \sum_{x \in X} \left(1 - \prod_{j=1}^{l} I\{x \cap M_j = \varnothing\}\right)$$

и моделирует значения p и η посредством формул $p = 1-(1-\xi)^D$, $\eta = \mathbf{E}\,(1-(1-\xi)^D)$.

В следующей теореме оценивается близость случайной величины p к некоторой оценке своего среднего значения.

Теорема. *Пусть*

$$\alpha = \frac{2\,(2f^{[1]} + f^{[2]})\,l}{N^2}, \quad \beta = 2\,f^{[2]}\,\frac{l^2}{N^2}.$$

Тогда

$$\mathbf{P}\left\{\left|\ln(1-\xi)^D - \ln e^{-Dlf^{[1]}/N}\right| > \varepsilon\right\} \leqslant \frac{D^2\alpha}{\varepsilon^2}\,\frac{(9+2\alpha)}{e^{-2lf^{[1]}/N}} + \left(\mathrm{ch}\left(\frac{\varepsilon}{D}\right) - 1\right).$$

В соответствии с результатом данной теоремы для приблизительных расчетов надежности в HM- и DP- методах при случайно сгенерированных таблицах следует брать величину $\eta \approx 1 - e^{-D\,l\,f^{[1]}/N}$.

СПИСОК ЛИТЕРАТУРЫ

1. Словарь криптографических терминов./ Под ред. Б. А. Погорелова, В. Н. Сачкова. М.: МЦНМО, 2006, 94 с.
2. *Hellman M. E.* A cryptanalytic time-memory trade-off. — IEEE Trans. Inform. Theory, 1980, v. IT-26, is. 4, p. 401–406.

3. *Borst J.*, *Preneel B.*, *Vandewalle J.* On the time-memory trade-off between exhaustive key search and table precomputation. — In: Nineteenth Symposium on Information Theory in the Benelux (Veldhoven, Netherlands, May 28–29, 1998)./ Ed. by P.H.N. de With, M. v.d. Schaar-Mitrea. Enschede: Werkgemeenschap voor informatie- en Communicatietheorie, 1998, p. 111–118.
4. *Standaert F. X.*, *Rouvroy G.*, *Quisquater J. J.*, *Legat J. D.* A time-memory tradeoff using distinguished points: New analysis & FPGA results. — In: Cryptographic Hardware and Embedded Systems — CHES 2002. 4th International Workshop. (Redwood Shores, CA, August 13–15, 2002.) Proceedings./ Ed. by B. S. Kaliski Jr., C. K. Koc, C. Paar. N. Y. etc.: Springer, 2003, p. 596–611. (Ser. Lect. Notes Comput. Sci. V. 2523.)
5. *Oechslin Ph.* Making a faster cryptanalytic time-memory trade-off. — In: Advances in Cryptology — CRYPTO'03. 23rd Annual International Cryptology Conference. (Santa Barbara, CA, August 17–21, 2003.) Proceedings./ Ed. by D. Boneh. N. Y. etc.: Springer, 2003, p. 617–630. (Ser. Lect. Notes Comput. Sci. V. 2729.)