

В. О. Миронкин (Москва, МИРЭА). Оценка снизу средней трудоемкости алгоритма опробования ключа до успеха для одной модели дискретного источника формирования ключей.

УДК 519.218+004.056.5 DOI https://doi.org/10.52513/08698325_2024_31_1_1

Резюме: Для математической модели двоичного дискретного источника, описывающего реальные физические устройства, используемые для формирования ключей, получена компактная и легко вычисляемая оценка снизу для средней трудоемкости алгоритма опробования ключа до успеха.

Ключевые слова: Алгоритм опробования ключа до успеха.

Общие сведения

В соответствии с [1] рассмотрим двоичный дискретный источник — вероятностное пространство $(\{0, 1\}^\infty, \mathcal{F}, \mathbf{P})$, где $\mathcal{F}$ — наименьшая по включению σ -алгебра на $\{0, 1\}^\infty$, содержащая все цилиндрические множества [2] общего вида, а вероятность $\mathbf{P}$ такова, что для ее конечномерных распределений $P_{t_1, t_2, \dots, t_k}$, $1 \leq t_1 < t_2 < \dots < t_k$, $k = 1, 2, \dots$, выполняется соотношение

$$\left(\frac{1}{2} - \varepsilon\right)^k \leq P_{t_1, t_2, \dots, t_k}(x_1, x_2, \dots, x_k) \leq \left(\frac{1}{2} + \varepsilon\right)^k \quad (1)$$

для произвольных $(x_1, x_2, \dots, x_k) \in \{0, 1\}^k$, где $0 \leq \varepsilon \leq \frac{1}{2}$, а последовательность элементов $t_1, t_2, \dots, t_k$ определяет моменты времени формирования источником $(\{0, 1\}^\infty, \mathcal{F}, \mathbf{P})$ знаков $x_1, x_2, \dots, x_k$.

В работе [1] для источника (1), формирующего ключи в соответствии с вероятностной схемой

$$\mathcal{A}_\varepsilon(\bar{t}) \sim \begin{pmatrix} \omega_1 & \omega_2 & \dots & \omega_{2^n} \\ p_1(\bar{t}) & p_2(\bar{t}) & \dots & p_{2^n}(\bar{t}) \end{pmatrix}, \quad (2)$$

где $\omega_j \in \{0, 1\}^n$, $j = 1, 2, \dots, 2^n$, а компоненты вектора $\bar{p}(\bar{t}) = (p_1(\bar{t}), p_2(\bar{t}), \dots, p_{2^n}(\bar{t}))$ удовлетворяют системе соотношений

$$\begin{cases} p_1(\bar{t}) + p_2(\bar{t}) + \dots + p_{2^n}(\bar{t}) = 1, \\ 1 > p_1(\bar{t}) \geq p_2(\bar{t}) \geq \dots \geq p_{2^n}(\bar{t}) > 0, \\ \left(\frac{1}{2} - \varepsilon\right)^n \leq p_j(\bar{t}) \leq \left(\frac{1}{2} + \varepsilon\right)^n, \quad j = 1, 2, \dots, 2^n, \end{cases} \quad (3)$$

получена достижимая оценка снизу средней трудоемкости алгоритма опробования ключа до успеха:

$$T_n^{(1)}(\varepsilon) = s + 1 + (2^n - s - 1) \frac{2^n - s}{2} \left(\frac{1}{2} - \varepsilon\right)^n - \frac{s(s+1)}{2} \left(\frac{1}{2} + \varepsilon\right)^n, \quad (4)$$

где $s = \left\lfloor 2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n} \right\rfloor$, а $n \in \mathbb{N}$ и ε , $0 < \varepsilon < \frac{1}{2}$ — произвольные и определяются вероятностной схемой (2).

З а м е ч а н и е 1. Характеристика $T_n^{(1)}(\varepsilon)$ играет особую практическую роль при решении целого ряда задач информационной безопасности [3, 4, 5], в том числе при синтезе и анализе аппаратно-программных средств, используемых для генерации случайных последовательностей [6], на основе которых формируются ключи шифрования, ключи электронной подписи, пароли, пин-коды и т. д.

Отметим, что оценка (4) является достижимой, имеет достаточно простой аналитический вид и эффективна вычислима при больших значениях $n \in \mathbb{N}$, используемых в ряде практических приложений. Однако и ее можно упростить без существенной потери точности оценивания.

Основной результат

Утверждение 1. Для произвольных $n \in \mathbb{N}$ и ε , $0 < \varepsilon < \frac{1}{2}$, справедливо неравенство

$$T_n^{(1)}(\varepsilon) \geq \tilde{T}_n^{(1)}(\varepsilon) = 2^{n-1} \frac{1 - 2(1-2\varepsilon)^n + (1-4\varepsilon^2)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n} + \frac{1}{2}. \quad (5)$$

При этом $0 \leq T_n^{(1)}(\varepsilon) - \tilde{T}_n^{(1)}(\varepsilon) < \frac{1}{8}$.

Д о к а з а т е л ь с т в о. Для произвольных фиксированных $n \in \mathbb{N}$ и ε , $0 < \varepsilon < \frac{1}{2}$, положим

$$\omega = 2^n \frac{1 - (1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n} - s \quad (6)$$

и построим сначала оценку снизу $\hat{T}_n^{(1)}(\varepsilon)$ для $T_n^{(1)}(\varepsilon)$, исключив из (4) целую часть выражения $2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n}$ путем замены величины s в ее первом вхождении в (4) на выражение $2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n} - 1 = s + \omega - 1$, а во всех остальных вхождениях — на $2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n} = s + \omega$:

$$\begin{aligned} T_n^{(1)}(\varepsilon) &\geq \hat{T}_n^{(1)}(\varepsilon) \\ &= s + \omega + (2^n - s - \omega - 1) \frac{2^n - s - \omega}{2} \left(\frac{1}{2} - \varepsilon\right)^n - \frac{(s + \omega)(s + \omega + 1)}{2} \left(\frac{1}{2} + \varepsilon\right)^n. \end{aligned}$$

Далее путем несложных преобразований, учитывая, что по определению величины s (см. [1]), где $s < 2^n$, совпадающей с наибольшим натуральным числом, удовлетворяющим условию

$$s \left(\frac{1}{2} + \varepsilon \right)^n + (2^n - s) \left(\frac{1}{2} - \varepsilon \right)^n \leq 1, \quad (7)$$

следует равенство

$$(s + \omega) \left(\frac{1}{2} + \varepsilon \right)^n + (2^n - s - \omega) \left(\frac{1}{2} - \varepsilon \right)^n = 1, \quad (8)$$

получим следующую цепочку соотношений:

$$\begin{aligned} T_n^{(1)}(\varepsilon) - \widehat{T}_n^{(1)}(\varepsilon) &= s + 1 + (2^n - s - 1) \frac{2^n - s}{2} \left(\frac{1}{2} - \varepsilon \right)^n - \frac{s(s+1)}{2} \left(\frac{1}{2} + \varepsilon \right)^n \\ &\quad - \left(s + \omega + (2^n - s - \omega - 1) \frac{2^n - s - \omega}{2} \left(\frac{1}{2} - \varepsilon \right)^n \right. \\ &\quad \left. - \frac{(s + \omega)(s + \omega + 1)}{2} \left(\frac{1}{2} + \varepsilon \right)^n \right) \\ &= 1 - \omega + \left(\frac{1}{2} + \varepsilon \right)^n (2s + \omega + 1) \frac{\omega}{2} + \left(\frac{1}{2} - \varepsilon \right)^n (2^{n+1} - 2s - \omega - 1) \frac{\omega}{2} \\ &= 1 - \omega + \left(\frac{1}{2} + \varepsilon \right)^n (2s + 2\omega) \frac{\omega}{2} + \left(\frac{1}{2} - \varepsilon \right)^n (2^{n+1} - 2s - 2\omega) \frac{\omega}{2} \\ &\quad - \left(\frac{1}{2} + \varepsilon \right)^n (\omega - 1) \frac{\omega}{2} + \left(\frac{1}{2} - \varepsilon \right)^n (\omega - 1) \frac{\omega}{2} \\ &= 1 - \frac{\omega(\omega - 1)}{2} \left(\left(\frac{1}{2} + \varepsilon \right)^n - \left(\frac{1}{2} - \varepsilon \right)^n \right). \end{aligned}$$

В соответствии с (6) величина ω представляет собой дробную часть числа $s + \omega$, и поэтому $0 \leq \omega < 1$. Кроме того, на полуинтервале $[0, 1)$ величина $\frac{\omega(\omega-1)}{2} \in [-\frac{1}{8}, 0]$. Таким образом,

$$1 \leq T_n^{(1)}(\varepsilon) - \widehat{T}_n^{(1)}(\varepsilon) \leq 1 + \frac{1}{8} \left(\left(\frac{1}{2} + \varepsilon \right)^n - \left(\frac{1}{2} - \varepsilon \right)^n \right) < \frac{9}{8}.$$

Теперь, взяв в качестве искомой оценки величину $\widetilde{T}_n^{(1)}(\varepsilon) = \widehat{T}_n^{(1)}(\varepsilon) + 1$, получим неравенство

$$0 \leq T_n^{(1)}(\varepsilon) - \widetilde{T}_n^{(1)}(\varepsilon) < \frac{1}{8}.$$

При этом, учитывая (8), приходим к представлению (5) для оценки

$\tilde{T}_n^{(1)}(\varepsilon):$

$$\begin{aligned}
 \tilde{T}_n^{(1)}(\varepsilon) &= s + \omega + 1 + (2^n - s - \omega - 1) \frac{2^n - s - \omega}{2} \left(\frac{1}{2} - \varepsilon\right)^n \\
 &\quad - \frac{(s + \omega)(s + \omega + 1)}{2} \left(\frac{1}{2} + \varepsilon\right)^n = 2^n \frac{2^n - s - \omega}{2} \left(\frac{1}{2} - \varepsilon\right)^n \\
 &\quad + \frac{s + \omega + 1}{2} \left(2 - (2^n - s - \omega) \left(\frac{1}{2} - \varepsilon\right)^n - (s + \omega) \left(\frac{1}{2} + \varepsilon\right)^n\right) \\
 &= \frac{s + \omega}{2} (1 - (1 - 2\varepsilon)^n) + 2^{n-1} (1 - 2\varepsilon)^n + \frac{1}{2} \\
 &= 2^{n-1} \frac{1 - 2(1 - 2\varepsilon)^n + (1 - 4\varepsilon^2)^n}{(1 + 2\varepsilon)^n - (1 - 2\varepsilon)^n} + \frac{1}{2}.
 \end{aligned}$$

Утверждение доказано. ■

В заключение отметим, что для наиболее часто применяемых на практике значений $n \in \mathbb{N}$ построенная оценка $\tilde{T}_n^{(1)}(\varepsilon)$ имеет высокую точность. Так, например, для $n = 256$ и $\varepsilon = 10^{-2}$ эталонная достижимая снизу оценка $T_n^{(1)}(\varepsilon)$ имеет порядок 10^{74} , что не соизмеримо с величиной отклонения $\frac{1}{8}$.

СПИСОК ЛИТЕРАТУРЫ

1. *Логачев А. С., МIRONKIN В. О.* О влиянии вероятностных характеристик дискретных источников, формирующих криптографические ключи, на практическую секретность ключа. — Прикладная дискретн. матем., 2024, в. 65, с. 66–83. // *Logachev A. S., Mironkin V. O.* O vliyaniy veroyatnostnykh kharakteristik diskretnykh istochnikov, formiruyuchikh kriptograficheskie klyuchi, na prakticheskuyu sekretnost klyucha'. — Prikladnaya diskretnaya matematika, 2024, is. 65, p. 66–83. (in Russian).
2. *Лось А. Б., МIRONKIN В. О.* Теоретико-информационные аспекты защиты информации, М.: URSS, 2023, 144 с. // *Los A. B., Mironkin V. O.*, Teoretiko-informacionnye aspekty zashity informacii, М.: URSS, 2023, 144 с. (in Russian).
3. *Арбеков И. М.* Критерии секретности ключа. — Матем. вопросы криптографии, 2016, т. 7, в. 1, с. 39–56. // *Arbekov I. M.*, Kriterii sekretnosti klucha. — Matem. Vopr. kriptografii, 2016, v. 7, is. 1, p. 39–56 (in Russian).
4. *Arbekov I. M.* Lower bounds for the practical secrecy of a key. — Matem. Vopr. Kriptogr., 2017, v. 8, is. 2, p. 29–38.
5. *Арбеков И. М.* Элементарная квантовая криптография: Для криптографов, не знакомых с квантовой механикой, М.: URSS, 2022, 168 с. // *Arbekov I. M.*, Elementarnaya kvantovaya kriptografiya: Dlya kriptografov, ne znakomyh s kvantovoy mekhanikoy, М.: URSS, 2022, 168 p. (in Russian).
6. *Turam M., Barker E., Kelsey J., McKay K.* Recommendation for the Entropy Sources Used for Random Bit Generation, NIST Special Publication 800-90B, 2018, 76 p.

Поступила в редакцию
02.VII.2024

UDC 519.218+004.056.5

DOI https://doi.org/10.52513/08698325_2024_31_1_1

Mironkin V O.* (Moscow, MIREA). **The lower estimate of the average complexity of the algorithm of testing a key to success for one model of a discrete source of key generation.*

Abstract: For a mathematical model of a binary discrete source describing real physical devices used to generate keys, a compact and easily computable lower estimate is obtained for the average complexity of the algorithm of testing a key to success.

Keywords: Algorithm of testing a key to success.