ОЦЕНКА КАЧЕСТВА КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ МАЛОПАРАМЕТРИЧЕСКИХ МОДЕЛЕЙ

Мальцев М. В.

БГУ, НИИ прикладных проблем математики и информатики,
Минск, Беларусь,e-mail: maltsew@bsu.by

Криптографические методы защиты информации широко применяются для обеспечения безопасности коммуникаций в Интернете. К примеру, данные, передаваемые через Интернет, могут быть зашифрованы с помощью протоколов SSL и TLS. Для надежного шифрования необходимы криптографические генераторы – устройства, генерирующие случайные или псевдослучайные последовательности. Выходная последовательность генератора представляет собой дискретный временной ряд, поэтому для оценки качества криптографических генераторов используются статистические методы. Известной универсальной моделью дискретных временных рядов является конечная однородная цепь Маркова порядка s, $s < \infty$. К сожалению, число независимых параметров этой модели возрастает экспоненциально с увеличением порядка, что затрудняет ее непосредственное применение на практике. Для решения этой проблемы разрабатываются малопараметрические модели – частные случаи цепи Маркова порядка s, которые задаются значительно меньшим числом параметров. К малопараметрическим моделям относится рассматриваемая в статье цепь Маркова условного порядка и ее обобщения.

Приведем описание этой математической модели согласно [1]. Обозначим: $\mathbf{N}$ – множество натуральных чисел; $A = \{0, 1,..., N-1\}$ – пространство состояний мощности $N \in \mathbf{N}$, $2 \le N < \infty$; $J_n^m = (j_n, j_{n+1},..., j_m) \in A^{m-n+1}$, $m, n \in \mathbf{N}$, $m \ge n$, – мультииндекс; $\mathrm{I}\{B\}$ – индикаторная функция события B; $\{x_t \in A : t \in \mathbf{N}\}$ – однородная цепь Маркова s-го порядка ($2 \le s < \infty$) с вероятностями одношаговых переходов $p_{J_1^{s+1}} = \mathrm{P}\{x_{t+s} = j_{s+1} \mid X_t^{t+s-1} = J_1^s\}$, $J_1^{s+1} \in A^{s+1}$; $1 \le L \le s-1$, $K = N^L - 1$ – натуральные числа; $Q^{(1)},..., Q^{(M)}$ – M ($1 \le M \le K+1$) различных квадратных стохастических матриц порядка N. Цепь Маркова s-го порядка $\{x_t \in A : t \in \mathbf{N}\}$ называется цепью Маркова условного порядка, если ее вероятности одношаговых переходов имеют вид:

$$p_{J_1^{s+1}} = \sum_{k=0}^{K} \mathrm{I}\left\{ \sum_{i=s-L+1}^{s} N^{i-s+L-1} j_i = k \right\} q_{j_{b_k} j_{s+1}}^{(m_k)}, \; J_1^{s+1} \in A^{s+1}, \qquad (1)$$

где $1 \le m_k \le M$, $1 \le b_k \le s-L$, $\min\limits_{0 \le k \le K} b_k = 1$. Цепочка из L элементов J_{s-L+1}^{s} называется базовым фрагментом памяти (БФП), величина $s_k = s - b_k + 1$ – условным порядком.

На основе представленной модели построены алгоритмы статистического тестирования и распознавания криптографических генераторов. Разработаны два обобщения модели (1): в первом случае используется БФП, распределенный по всей глубине памяти, во втором матрицы $Q^{(1)},...,Q^{(M)}$ являются многомерными.

Литература