Алгоритмы. Большое внимание уделено выбору оптимальных арифметических алгоритмов. Были проведены достаточно подробные вычислительные эксперименты, а их результаты учтены в окончательных редакциях программ. Например, при создании кольца классов вычетов целых чисел по модулю m реализуется следующая основанная на экспериментах стратегия выбора функции редукции $x \to x \bmod m$: если m имеет вид $2^{nw} - c$, где w – длина машинного слова, $n \geq 2$ и $c < 2^w$, то используется редукция Крэндалла; иначе, если m – нечетное, – редукция Монтгомери; иначе, если $m > 2^{4w}$, – редукция Барретта, иначе – обычная редукция через деление уголком.

Разработано несколько новых алгоритмов арифметики больших чисел, например, алгоритм деления большого числа на машинное слово, в котором каждое деление машинных слов заменяется на два умножения. На многих процессорах этот алгоритм работает намного быстрее обычного.

В функциях работы с машинными словами активно применяются алгоритмические трюки из прекрасной книги [1].

Алгебраическая абстракция. Работа с алгебраическими структурами реализована через довольно общие, но достаточно насыщенные интерфейсы. Например, интерфейс qr описывает работу с абстрактным кольцом вычетом по модулю его идеала. Предусмотрены функции сложения, вычитания, аддитивного обращения, умножения, возведения в квадрат, мультипликативного обращения, деления, экспорта в строку октетов и импорта из такой строки. Реализация всех функций интерфейса не обязательна. В Bee2 интерфейс qr инстанциируется многими способами: zm – кольцо вычетов целых чисел, pp – кольцо многочленов, gfp – простое поле из $p > 2$ элементов, gf2 – поле характеристики 2. Арифметика эллиптических кривых описывается интерфейсов ec, который является надстройкой над qr.

Доверие. Главный фактор доверия к криптографической программе – открытые исходные тексты. Библиотека Bee2 является открытым программным обеспечением, распространяется на условиях GNU General Public License версии 3. Исходные тексты размещены по адресу https://github.com/agievich/bee2.

Список использованных источников

1. *Уоррен, Генри Мл.* Алгоритмические трюки для программистов / Генри Мл. Уоррен. – М.: Изд. дом «Вильямс», 2003.

МАЛОПАРАМЕТРИЧЕСКИЕ МАРКОВСКИЕ МОДЕЛИ ДЛЯ ОПИСАНИЯ СЛОЖНЫХ ЗАВИСИМОСТЕЙ В ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ

М. В. МАЛЬЦЕВ

Цепь Маркова условного порядка (ЦМУП) – математическая модель, разработанная в НИИ прикладных проблем математики и информатики БГУ для описания сложных зависимостей, возникающих в псевдослучайных последовательностях [1; 2]. Эта модель относится к классу так называемых малопараметрических марковских моделей, которые строятся на основе цепи Маркова высокого порядка. Число параметров, необходимое для задания матрицы вероятностей одношаговых переходов цепи Маркова порядка s с N состояниями, составляет $N^s(N–1)$. Данное обстоятельство ограничивает практическое использование этой универсальной модели сравнительно небольшими значениями s. В связи с этим для поиска зависимостей большой глубины в выходных последовательностях криптографических генераторов применяются малопараметрические модели [3], представляющие собой цепь Маркова порядка s, матрица вероятностей одношаговых переходов которой имеет специальный вид. Число параметров для таких моделей не возрастает экспоненциально

с ростом порядка, поэтому становится возможным использовать на практике значения $s \geq 100$.

На основе ЦМУП разработаны алгоритмы идентификации и распознавания криптографических генераторов; построен алгоритм статистического тестирования, который позволяет обнаруживать зависимости большой глубины в псевдослучайных последовательностях [1; 2]. В данной статье предлагаются два обобщения модели ЦМУП, представлены результаты вычислительных экспериментов.

Вначале приведем определение ЦМУП. Обозначим: $\mathbf{N}$ – множество натуральных чисел; $A = \{0, 1,..., N-1\}$ – пространство состояний мощности $N \in \mathbf{N}$, $2 \leq N < \infty$; $J_n^m = (j_n, j_{n+1},..., j_m) \in A^{m-n+1}$, $m, n \in \mathbf{N}$, $m \geq n$, – мультииндекс; $< J_n^m > = \sum_{k=n}^{m} N^{k-n} j_k$ – числовое представление мультииндекса J_n^m; $\mathrm{I}\{B\}$ – индикаторная функция события B; $\{x_t \in A : t \in \mathbf{N}\}$ – однородная цепь Маркова s-го порядка ($2 \leq s < \infty$) с вероятностями одношаговых переходов $p_{J_1^{s+1}} = \mathrm{P}\{x_{t+s} = j_{s+1} \mid X_t^{t+s-1} = J_1^s\}$, $J_1^{s+1} \in A^{s+1}$; $1 \leq L \leq s-1$, $K = N^L - 1$ – натуральные числа; $Q^{(1)},..., Q^{(M)} - M$ ($1 \leq M \leq K+1$) 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:

$$p_{J_1^{s+1}} = \sum_{k=0}^{K} \mathrm{I}\{< J_{s-L+1}^s >= k\} q_{j_{b_k}, j_{s+1}}^{(m_k)}, \quad J_1^{s+1} \in A^{s+1}, \tag{1}$$

где $1 \leq m_k \leq M$, $1 \leq b_k \leq s-L$, $\min\limits_{0 \leq k \leq K} b_k = 1$. Цепочка из L элементов J_{s-L+1}^s называется *базовым фрагментом памяти* (БФП), величина $s_k = s - b_k + 1$ – *условным порядком.* Таким образом, распределение вероятностей состояния процесса в момент времени t зависит не от всех s предыдущих состояний, как это было бы для полносвязной цепи Маркова порядка s, а от $L+1$ состояний (j_{b_k}, J_{s-L+1}^s). Число параметров модели (1) составляет $2(N^L + 1) + MN(N-1)$. Отметим, что при $L = s-1$, $s_0 = ... = s_K = s$, получаем полносвязную цепь Маркова порядка s.

Обобщения модели (1) возможны по двум направлениям:

- использование обобщенного базового фрагмента памяти;
- использование многомерных матриц $Q^{(1)},..., Q^{(M)}$.

Дадим краткое описание этих обобщений. Обозначим: $W = \{1,..., s\}$; $W_L = (w_1,..., w_L)$, $1 \leq w_1 < ... < w_L \leq s$, – вектор длины L с упорядоченными по возрастанию компонентами; $\mathbf{W}$ – множество всех таких векторов; $W_L^+ = (w_1,..., w_L, s+1)$; $\overline{W} = W \setminus \{w_1,..., w_L\}$. Цепь Маркова s-го порядка $\{x_t \in A : t \in \mathrm{N}\}$ назовем цепью Маркова условного порядка с обобщенным базовым фрагментом памяти W_L, если ее вероятности одношаговых переходов имеют вид

$$p_{J_1^{s+1}} = \sum_{k=0}^{K} \mathrm{I}(< S(J_1^s, W_L) >= k) q_{j_{b_k}, j_{s+1}}^{(m_k)}, \tag{2}$$

где S – функция-селектор: $S(J_1^s, W_L) = (j_{w_1},..., j_{w_L})$. Отличие данной модели от ЦМУП (1) состоит в дополнительном параметре $W_L = (w_1,..., w_L)$ – обобщенном БФП, распределенном по всей глубине памяти s. Если $W_L = \{s-L+1,..., s\}$, то (2) преобразуется в (1) и в этом частном случае приходим к введенной ранее модели. Число независимых параметров для цепи Маркова с обобщенный БФП равно $2(N^L + 1) + MN(N-1) + L$.

В рамках второго направления обобщения цепи Маркова условного порядка вероятности переходов при фиксированном БФП определяются не одним дополнительным состоянием j_{b_k}, а несколькими, матрицы вероятностей одношаговых переходов при этом являются многомерными. Соотношение (1) для такой

модели, называемой цепью Маркова обобщенного условного порядка, имеет следующий вид:

$$p_{j_1^{s+1}} = \sum_{k=0}^{K} \mathrm{I}(< J_{s-L+1}^{s} >= k) q^{(m_k)}_{j_{b_k^{(1)}},\ldots,j_{b_k^{(r)}},j_{s+1}}, \qquad (3)$$

где $\overline{Q}^{(m_k)} = (q^{(m_k)}_{j_{b_k^{(1)}},\ldots,j_{b_k^{(r)}},j_{s+1}})$ – $(r+1)$-мерная матрица вероятностей одношаговых переходов, $1 \le r \le s-L$; $\{b_k^{(1)},\ldots, b_k^{(r)}\} \subseteq \{1,\ldots, s-L\}$ – множество r различных элементов. Отличие от цепи Маркова условного порядка (1) состоит в том, что условные порядки, определяющие распределение вероятностей будущего состояния цепи Маркова, являются векторами длины r. Поэтому вместо двумерных матриц $Q^{(m_k)}$ используются матрицы $\overline{Q}^{(m_k)}$ размерности $r+1$. Таким образом, если $r = 1$, то (3) преобразуется в исходную модель (1). Число независимых параметров для цепи Маркова обобщенного условного порядка составляет $N^L(r+1) + MN^r(N-1) + 2$.

Далее будем рассматривать первый тип обобщений – ЦМУП с обобщенным БФП.

Обозначим: $A_{W_L,y}(J_0^L) = \{I_1^{s+1} \in A^{s+1} : i_y = j_0,\ i_{w_1} = j_1,\ldots,\ i_{w_L} = j_L\},\ y \in \overline{W}$, – подмножество $(s+1)$-грамм с фиксированными значениями $j_0, j_1, \ldots, j_L$ на позициях $y, \omega_1, \ldots, \omega_L$ соответственно, $\nu_{W_L,y}(J_0^L) = \sum_{I_1^{s+1} \in A_{W_L,y}(J_0^L)} \sum_{t=1}^{n-s} \mathrm{I}\{X_t^{t+s} = J_1^{s+1}\}$ – частота фрагмента J_0^L с пропусками, определяемыми параметрами y и W_L. Аналогично определяются $A_{W_L^+,y}(J_0^{L+1})$ и $\nu_{W_L^+,y}(J_0^{L+1})$.

Для параметров ЦМУП с обобщенным БФП построены оценки максимального правдоподобия (ОМП).

Теорема 1. Если истинные значения параметров L, $\{b_k\}$, W_L, $\{m_k = k+1\}$ известны, то ОМП вероятностей одношаговых переходов $q^{(k+1)}_{j_0,j_{L+1}}$, $j_0, j_{L+1} \in A$, $k = 0,\ldots, K$, имеют вид

$$q^{(k+1)}_{j_0,j_{L+1}} = \begin{cases} \sum_{J_1^L \in A^L} \mathrm{I}\{< J_1^L >= k\} \dfrac{\nu_{W_L^+,b_k}(J_0^{L+1})}{\nu_{W_L,b_k}(J_0^L)}, \text{ если } \nu_{W_L,b_k}(J_0^L) > 0, \\ 1/N, \text{ если } \nu_{W_L,b_k}(J_0^L) = 0. \end{cases}$$

Теорема 2. Если истинные значения L, W_L, $\{m_k = k+1\}$ известны, то ОМП условных порядков $\{s_k\}$ имеют вид

$$\hat{s}_k = \arg\max_{y \in \overline{W}} \sum_{j_0,j_{L+1} \in A} \nu_{W_L^+,s-y+1}(J_0^{L+1}) \ln(\hat{q}^{(k+1)}_{j_0,j_{L+1}}),\ < J_1^L >= k,\ k = 1,\ldots,K. \qquad (4)$$

Теорема 3. Если истинное значение L известно, то ОМП обобщенного БФП W_L имеет вид:

$$\hat{W}_L = \arg\max_{U_L = (u_1,\ldots,u_L) \in \mathrm{W}} \sum_{J_0^{L+1} \in A^{L+2}} \nu_{U_L^+,s-\hat{s}_k+1}(J_0^{L+1}) \ln(\hat{q}^{(k+1)}_{j_0,j_{L+1}}),\ < J_1^L >= k,\ k = 0,\ldots,K. \qquad (5)$$

Представим теперь результаты компьютерных экспериментов на реальных данных, использующие полученные теоремы. Исследовались выходные последовательности генератора с динамическим изменением закона рекурсии [4]. Генератор построен на основе регистра сдвига с линейной обратной связью. На четных тактах для генерации выходного бита используется характеристический многочлен $f_0(x)$, на нечетных – $f_1(x)$. В компьютерных экспериментах многочлены принимали следующие значения: $f_0(x) = x^{49} + x^9 + 1$, $f_1(x) = x^{49} + x^{22} + 1$. В ходе экспериментов решалась задача восстановления значения характеристических многочленов $f_0(x)$ и $f_1(x)$ по выходной последовательности при известной длине регистра; также полагалось известным, что характеристические многочлены являются триномами. Таким образом, для решения

этой задачи требовалось при известных s и L оценить условные порядки s_k и обобщенный БФП W_L с помощью формул (4) и (5) соответственно. Компьютерные эксперименты проводились по следующей схеме. Генерировалось U = 1000 реализаций выходной последовательности генератора с динамическим изменением закона рекурсии длительности $100 \le n \le 50000$ со случайно выбранным начальным заполнением регистров. Для каждой реализации вычислялась величина $\delta_u(n) \in \{0, 1\}$, где $1 \le u \le U$ – номер реализации; $\delta_u(n) = 1$, если характеристические многочлены восстановлены верно (что соответствует $\hat{W}_L = (1)$, $(\hat{s}_0, \hat{s}_0) \in \{(10, 23),(23,10)\}$, в противном случае $\delta_u(n) = 0$. По результатам всех U экспериментов вычислялась величина

$$\Delta(n) = \frac{1}{U}\sum_{u=1}^{U}\delta_u(n),$$

характеризующая частоту правильного восстановления характеристических многочленов.

В таблице 1 приведены значения $\Delta(n)$ при различных значениях длительности выходной последовательности генератора.

Таблица 1

Зависимость $\Delta(n)$ от n

n	100	500	1000	2000	5000	10000	20000	30000	50000
Δ(n)	0.185	0.855	0.894	0.934	0.963	0.960	0.977	0.982	0.981

Таким образом, результаты вычислительных экспериментов демонстрируют применимость цепей Маркова условного порядка для выявления зависимостей большой глубины в псевдослучайных последовательностях: даже при длине выходной последовательности 500 бит более 85 % реализаций были идентифицированы верно.

Список использованных источников

1. *Мальцев, М. В.* О выявлении зависимостей большой глубины в псевдослучайных последовательностях на основе цепи Маркова условного порядка / М. В. Мальцев // Электроника ИНФО. – 2013. – № 6. – С. 202–207.

2. *Kharin, Yu. S.* Markov chain of conditional order: properties and statistical analysis / Yu.S. Kharin, M.V. Maltsew // Austrian Journal of Statistics. – 2014. – Vol. 43, № 3–4. – P. 205–216.

3. *Харин, Ю. С.* Оптимальность и робастность в статистическом прогнозировании / Ю. С. Харин. – Минск: БГУ, 2008. – 263 с.

4. Основы криптографии / А. П. Алферов [и др.]. – М.: Гелиос АРВ, 2001. – 480 с.

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ СРЕДСТВ И МЕТОДОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (ОБЗОР ПО МАТЕРИАЛАМ ПОСЛЕДНИХ МЕЖДУНАРОДНЫХ КОНФЕРЕНЦИЙ)

В. В. КОМИСАРЕНКО

В докладе приводится обзорная информация по следующим направлениям.

1) ***теоретическая криптография:***

- симметричные алгоритмы;
- криптография с открытым ключом;
- квантовая криптография;
- стандартизация;

2) ***прикладная криптография:***

- криптографические средства на мобильных платформах;