времени получении данных об объектах — все необходимые сведения уже содержатся в test_name.log.

Таким образом, данный подход к функциональному тестированию решает проблемы, связанные с человеческим фактором, длительным временем проведения тестовых испытаний и большими вычислительными ресурсами, необходимыми для выполнения тестов. Автоматизация тестовых испытаний позволяет снять с человека ответственность за корректную интерпретацию результатов и выполнение всех тестов и позволяет сократить время тестирования, а разделение процесса тестирования на два независимых этапа позволяет сократить требуемые вычислительные ресурсы.

СПИСОК ЛИТЕРАТУРЫ

1. *Куликов С. С.* Тестирование программного обеспечения. Базовый курс: практ. пособие. Минск: Четыре четверти, 2015. С. 63–110
2. *Постоев Д. А.* Управление доступом в виртуальных системах на основе контроля информационных потоков // Безопасность информационных технологий. М., 2014. № 4. С. 86–91.
3. *Каннер (Борисова) Т. М., Кузнецов А. В., Обломова А. И.* Тестирование средств защиты информации // Информационная безопасность. Материалы XIII Международной конференции. Таганрог 2013. Часть. 1. С. 121–129.

О ПРОГНОЗИРОВАНИИ ДВОИЧНЫХ ВРЕМЕННЫХ РЯДОВ С ИСПОЛЬЗОВАНИЕМ NVIDIA CUDA

В.В. ПЬЯНОВ, Ю.С. ХАРИН,
НИИ ППМИ БГУ

Введение

Случайные последовательности и их генераторы являются неотъемлемыми элементами современных криптосистем [1]. Случайные последовательности используются для построения гаммы в поточных криптосистемах, сеансовых и других ключей в блочных криптосистемах. Отметим, что для криптографических приложений требуются равномерно распределенные случайные последовательности значительной длины. Поэтому возникает важная задача статистического тестирования таких последовательностей. Одним из направлений статистического тестирования является проверка свойства невозможности прогнозирования выходных последовательностей криптографических генераторов статистическими методами. В данной статье представляется эффективный вычислительный алгоритм статистического прогнозирования, основанный на нахождении оптимального шаблона прогнозирования в классе малопараметрических цепей Маркова высокого порядка.

Математическая модель временного ряда

Пусть на вероятностном пространстве (Ω, F, P) наблюдается двоичный временной ряд $x = (x_1,..,x_T) \in V^T = \{0,1\}^T, x_t \in V = \{0,1\}, t = 1,\ldots,T$, длины T, являющийся цепью Маркова порядка s, $s \gg 1$, обладающий следующим гипотетическим свойством:

$$\frac{1}{2}-\varepsilon \le \left| P\{x_t = j_0 | x_{t-1} = j_1, \ldots, x_{t-s} = j_s\} - \frac{1}{2} \right| \le \frac{1}{2},\ j_0, j_1, \ldots, j_s \in V, \qquad (1)$$

где $\varepsilon \in \left[0, \frac{1}{2}\right)$ — некоторое достаточно малое число. Это свойство означает, что при некотором достаточно большом s в выходной последовательности $\{x_t\}$ криптографического генератора существует статистически значимая зависимость глубины s. Прогнозированию подлежит последующий бит $x_{T+1} \in V$.

Так как распределение вероятностей, входящее в (1), на практике неизвестно, а его статистическое оценивание имеет вычислительную сложность порядка $O\left(2^{s+1}\right)$, то необходимы другие подходы к прогнозированию, использующие малопараметрические модели цепи Маркова высокого порядка[1–4]. Выберем в качестве такой модели цепь Маркова порядка s с r частичными связями[2].

Пусть $r \in \mathbb{N}, 1 \le r \le s$ — число связей, $M = \{m_1, m_2, \ldots, m_r\}$ — целочисленный -вектор с упорядоченными компонентами $1 \le m_1 \le m_2 \le \ldots \le m_r \le s$, который будем называть шаблоном, $P = (p_{j_0,\ldots,j_{s-1},j_s}), j_0, \ldots, j_s \in V$ — $(s+1)\times(s+1)$ матрица вероятностей одношаговых переходов цепи Маркова x_t:

$$p_{j_0,\ldots,j_{s-1},j_s} = P\{x_t = j_0 | x_{t-1} = j_1, \ldots, x_{t-s} = j_s\},$$

$Q = (q_{j_0,\ldots,j_{r-1},j_r}), j_0, \ldots, j_r \in V$ — некоторая $(r+1)\times(r+1)$ стохастическая матрица.

Цепь Маркова $x_t \in V$ принято называть цепью Маркова *s*-го порядка с r частичными связями и обозначать ЦМ(s,r), если ее вероятности одношаговых переходов допускают следующее малопараметрическое представление:

$$p_{j_0,\ldots,j_{s-1},j_s} = q_{j_0,j_{m_1},\ldots,j_{m_r}},\ j_0, \ldots, j_s \in V.$$

В дальнейшем будем считать, что двоичный временной ряд

$$x = (x_1, .., x_T) \in V^T = \{0,1\}^T, x_t \in V = \{0,1\}, t = 1, \ldots, T$$

является цепью Маркова *s*-го порядка с r частичными связями.

Алгоритм прогнозирования на основе ЦМ(s,r) и его реализация на NVIDIA CUDA

Выберем $r \in \mathbb{N}, 1 \le r \le s$ и зафиксируем произвольный упорядоченный набор r номеров координат шаблона $M = \{m_1, m_2, \ldots, m_r\}$, где $1 \le m_1 \le m_2 \le \ldots \le m_r \le s$. Введем в рассмотрение условную вероятность события:

$$p(r, j_0, M) ::= P\{x_{T+1} = j_0 | x_{T-m_1} = j_1, \ldots, x_{T-m_r} = j_r\},$$

где $j_1, \ldots, j_r \in V$ — фиксированные наблюдаемые значения $x_{t-m_1}, \ldots, x_{t-m_r}$. В силу (1) будем строить прогноз для x_t на основе $x_{T-m_1}, \ldots, x_{T-m_r}$. Согласно [3], оптимальная прогнозирующая статистика для модели ЦМ(s,r) примет вид:

$$\hat{x}_{T+1} = \arg\max_{j_0} p(r, j_0, M). \qquad (2)$$

Сложность вычисления прогнозирующей статистики (2) имеет порядок $O\left(T+2^{r+1}\right)$. Точность прогноза оценивается величиной[3]

$$\mathrm{p}_{+}\left(r,M\right):=\max_{j_0\in V}\mathrm{p}\left(r,j_0,M\right).$$

Точность прогнозирования можно увеличить, максимизируя по $r\in\left[r_{min},r_{max}\right]$ и шаблону[4]:

$$p_{+}\left(r;M\right)\to\max_{r,M}, \tag{3}$$

где $r_{min}\left(r_{max}\right)$ — минимальное (максимальное) возможное число связей.

Решением экстремальной задачи (3) будет являться набор r^{*},M^{*} наиболее информативных компонент шаблона. Если решать данную максимизации (3) перебором, то вычислительная сложность будет иметь порядок $O\left(C_s^r T+2^{r+1}\right)$. Для уменьшения вычислительной сложности будем использовать алгоритм последовательной максимизации, позволяющий приближенно решать задачу максимизации по M. Пусть r изменяется в пределах $1\le r_{min}\le r\le r_{max}\le s$. Решим задачу максимизации по M для $r=r_{min}$ перебором всех возможных шаблонов длины r_{min} и получим $M^{r_{min}}$. Затем будем последовательно увеличивать r, добавляя к $M^{r_{min}}$ ещё одну не задействованную компоненту:

$$M^{r_{min}}=\arg\max_{M}p_{+}\left(r,\mathrm{M}\right),$$

$$M^{r}=\arg\max_{m\in\{1,..,s\}\setminus M^{r-1}}p_{+}\left(r,(M^{r-1},m)\right).$$

И так далее увеличиваем r пока не достигнем $r=r_{max}$.

В качестве оценки M^{*} принимаем $M^{r_{max}}$. Подставляя M^{*} в (2), получаем оценку для будущего значения x_{T+1}.

Для эффективной реализации алгоритма использовалась технология NVIDIA CUDA [5], которая благодаря архитектуре SIMT позволяет эффективно производить перебор при решении экстремальных задач (3), (4).

Численные результаты

Параметр s, означающий порядок цепи Маркова (глубину стохастической зависимости), в представленном алгоритме предполагался известным. Отметим, что в [4] предложен метод статистического оценивания параметров s,r на основе байесовского информационного критерия и информационного критерия Акаике.

Для тестирования разработанного алгоритма по точности, характеризуемой вероятностью ошибки:

$$p_{\text{ош.}}=P\left\{\hat{x}_{T+1}\ne x_{T+1}\right\},$$

и вычислительной сложностью, характеризуемой затратами машинного времени $t_{маш.}=1$ для вычисления прогноза $\hat{x}_{T+1}$, проведены две серии компьютерных экспериментов.

В первой серии обрабатывалось 10 реализаций двоичного дискретного временного ряда длины $T=2^{15}$, порождаемого линейной рекуррентой:

$$x_t=x_{t-16}\oplus x_{t-14}\oplus x_{t-13}\oplus x_{t-11},$$

соответствующего модели ЦМ(s,r) при $s=16, r=4, M^*=\{11,13,14,16\}$ и удовлетворяющего свойству (1) при $\varepsilon=0$. При $r_{min}=3, r_{max}=6$ прогнозирование всех 10 реализаций произошло безошибочно: $\hat{p}_{ош.}=0$; время обработки одной реализации составило $t_{маш.}=1$ сек. Результаты обработки всех 10 реализаций представлены в таблице 1 (истинные компоненты шаблона в оценке $\hat{M}^{r_{max}}$ выделены жирным шрифтом).

Во второй серии обрабатывалось 10 реализаций двоичного дискретного временного ряда длины $T=2^{15}$, порождаемого нелинейной рекуррентой:

$$x_t = x_{t-1} \oplus x_{t-2} \oplus x_{t-8}x_{t-11} \oplus x_{t-10}x_{t-16},$$

соответствующего модели ЦМ(s,r) при $s=17, r=6, M^*=\{1,2,8,10,11,16\}$ и удовлетворяющего свойству (1) при $\varepsilon=0$. При $r_{min}=4, r_{max}=6$ прогнозирование всех 10 реализаций произошло безошибочно: $\hat{p}_{ош.}=0$; время обработки одной реализации составило $t_{маш.}=1.8$ сек. Результаты обработки всех 10 реализаций представлены в таблице 2.

Таблица 1

Результаты прогнозирования для первой серии

Номер эксперимента	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
x_{T+1}	0	1	1	0	1	0	1	1	0	1
$\hat{x}_{T+1}$	0	1	1	0	1	0	1	1	0	1
$\hat{M}^{r_{max}}$	**16,14, 13,11**, 10, 4	**16**,15, **14,13, 11**, 5	**16,14, 13,11**, 7, 4	**16,14, 13,11**, 10, 8	**16,14**, **13**,12, **11**, 9	**16,14, 13,11**, 9, 6	**16,14**, **13**,12, **11**, 4	**16**,15, **14,13, 11**, 8	**16,14, 13,11**, 9, 6	**16,14, 13,11**, 10, 7

Таблица 2

Результаты прогнозирования для второй серии

Номер эксперимента	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
x_{T+1}	1	0	1	0	0	1	0	0	1	1
$\hat{x}_{T+1}$	1	0	1	0	0	1	0	0	1	1
$\hat{M}^{r_{max}}$	**1, 2, 10,11**, 14, **16**	**1, 2**, 4, 9, **11, 16**	**1, 2**, **10,11**, 13, **16**	**1, 2**, 3, 5, **8, 10**	**1, 2**, 6, **8, 10,16**	**1, 2, 8,10**, 11,17	**1, 2, 11**,14, **16**, 17	**1, 2**, 5, **8**, **10,16**	**1, 2, 11**,12, 15, **16**	**1, 2**, 7, **8**, **10**, **11**

Таким образом, компьютерные эксперименты показали эффективность разработанного алгоритма прогнозирования.

ЛИТЕРАТУРА

1. Криптология / Ю. С. Харин [и др.]. — Минск: БГУ, 2014. — 512 с.
2. *Харин Ю. С.* Цепи Маркова с r-частичными связями и их статистическое оценивание / Ю. С. Харин // Доклады НАН Беларуси. — 2004. Т. 48, № 1. — С. 40–44.

3. *Харин Ю. С.* Оптимальность и робастность в статистическом прогнозировании: монография / Ю. С. Харин. — Минск: БГУ, 2008. — 263 с.
4. *Харин Ю. С., Петлицкий А. И.,* «Идентификация двоичной цепи Маркова s-го порядка с r частичными связями при наличии аддитивных искажений», Дискрет. матем., 22:4 (2010), 138–155
5. CUDA Toolkit documentation. http://docs.nvidia.com/
6. *Dubrova E.* A List of Maximum Period NLFSRs //IACR Cryptology ePrint Archive. — 2012. — Т. 2012. — С. 166.
7. *Ward R. W., Molteno T. C. A.* Table of linear feedback shift registers. — Electronics Group, University of Otago, 2012.

ДОВЕРЕННАЯ ЗАГРУЗКА И МЕНЕДЖМЕНТ ЛОГИЧЕСКИХ ДИСКОВ. РОСКОШЬ ИЛИ НЕОБХОДИМОСТЬ

Д. И. ДЕВЯТИЛОВ
МФТИ

В тезисах описывается система LVM и объясняется необходимость контроля целостности файлов на данных системах.

Парадигма доверенных вычислений начала развиваться с конца прошлого столетия. Наблюдая за эволюцией парадигмы (от функционально-замкнутой среды (ФЗС) до доверенного сеанса связи (ДСС)) [14], можно с уверенностью сказать, что основа — это концепция (доверенной вычислительной среды) ДВС, для создания которой одним из условий является наличие резидентного компонента безопасности (РКБ)[1]. РКБ осуществляет проверку целостности технических и программных средств ПК и может быть реализован в виде аппаратного модуля доверенной загрузки (АМДЗ). Доверенная загрузка — загрузка операционных систем (ОС) только с заранее определенных носителей и после успешного прохождения специальных процедур контроля целостности (КЦ) программных и аппаратных средств ПК [2]. Конечно же, уместно говорить не о доверенной загрузке ОС, а о доверенной загрузке загрузчика ОС, т. к. после прохождения процедур КЦ управление передается не коду ОС, а коду загрузчика [3]. Доверенная загрузка будет считаться выполненной только после успешного прохождения всех процедур КЦ.

В силу того, что информационные технологии постоянно развиваются, усовершенствуются старые и создаются новые программные и аппаратные компоненты, в частности, операционные и файловые системы, необходимо для обеспечения функций безопасности доверенной загрузки поддерживать появляющиеся удобства цивилизации, уметь с ними работать. Ответом на такой вызов становится как усовершенствование самих фундаментальных парадигм доверенных вычислений [8, 9] и новых взглядов на реализацию РКБ [6, 13], так и поддержка новых технологий в существующих и уже зарекомендовавших себя подходах [7].

Необходимость более гибкого управления памятью запоминающих устройств ПК подталкивает на создание новых систем управления дисковым пространством [10]. Часто возникает необходимость в разбиении или, наоборот, соединении отдельных блоков памяти жесткого диска, сохраняя при этом все установленные ОС, данные и программы. Плюс, не хочется прибегать к резервному копированию имеющихся фай-