БИБЛИОТЕКА ФУНКЦИЙ ТЕСТИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ ЦЕПЕЙ МАРКОВА С ЧАСТИЧНЫМИ СВЯЗЯМИ

А. И. Петлицкий

Белорусский государственный университет
«НИИ прикладных проблем математики и информатики»,
НИЛ математических методов защиты информации
пр-т Независимости, 4, к. 802, г. Минск, Беларусь
телефон: (+37517) 2095549; факс: (+37517) 2095104; e-mail: piatlitski@bsu.by
web: www.bsu.by

Разработана библиотека функций тестирования криптографических генераторов на основе цепей Маркова с частичными связями. Библиотека состоит из двух составных частей: модуль цепей Маркова *s*-го порядка с *r* частичными связями; модуль двоичных цепей Маркова с частичными связями при наличии аддитивных искажений. Библиотека обеспечивает выполнение следующих функций: оценивание параметров модели криптографического генератора; статистическое тестирование генератора.

Ключевые слова – библиотека функций, криптографический генератор, тестирование, цепь Маркова с частичными связями.

1 ВВЕДЕНИЕ

Проблема защиты информации затрагивает практически все сферы деятельности человека. Среди способов защиты информации важнейшим считается криптографический [1]. Надежность любой системы криптографической защиты информации в значительной степени определяется качеством используемых генераторов случайных и псевдослучайных последовательностей [2].

При оценке качества криптографических генераторов возникает необходимость в моделях дискретных временных рядов с зависимостью высокого порядка [3]. Одной из широко используемых моделей для таких дискретных временных рядов является цепь Маркова высокого порядка [4, 5]. Однако для цепи Маркова число параметров растет экспоненциально при увеличении порядка и для идентификации требуется иметь реализацию не всегда доступной на практике длины. В связи с этим актуальна проблема построения и анализа цепи Маркова высокого порядка, в которой матрица вероятностей одношаговых переходов задается небольшим числом параметров. К такому классу моделей относятся: цепь Маркова *s*-го порядка с *r* частичными связями [6], двоичная цепь Маркова с частичными связями при наличии аддитивных искажений [7].

Разработанные алгоритмы идентификации неискаженной и искаженной цепи Маркова с частичными связями [6, 7] реализованы в виде библиотеки функций для тестирования криптографических генераторов.

2 ОПИСАНИЕ СТРУКТУРЫ БИБЛИОТЕКИ

Библиотека функций тестирования криптографических генераторов состоит из двух составных частей.

Модуль цепей Маркова с частичными связями предоставляет функциональные возможности для оценивания параметров и статистического тестирования криптографических генераторов, содержащих зависимости высокого порядка. В модуле реализованы следующие функции:

- CalculationNu – вычисление частотных статистик цепи Маркова с частичными связями по наблюдаемой реализации [6];
- EstimationMuX – оценивание распределения вероятностей $(r+1)$-грамм (использует CalculationNu) [6];
- EstimationQ_X – оценивание матрицы одношаговых переходов Q цепи Маркова с частичными связями [6];
- EstimationH_X – оценивание условной энтропии (EstimationMuX);
- AlgorithmA1X – оценивание шаблона связей с помощью полного перебора (EstimationH_X) [6];
- AlgorithmA2X – оценивание шаблона связей с помощью наращивания начального заданного шаблона [6];
- CalculationBIC_X – вычисление байесовского информационного критерия (EstimationMuX);
- EstimationSR_X – оценивание порядка и числа связей (AlgorithmA1X, AlgorithmA2X, CalculationBIC_X) [6];
- FunctionPhi – приближенное вычисление значения функции распределения нормально закона;
- P_value – вычисление P-значения (FunctionPhi);
- TestMC – тест на основе частотных статистик цепи Маркова с частичными связями (EstimationMuX, P_value).

Модуль двоичных цепей Маркова с частичными связями при наличии аддитивных искажений включает процедуры для идентификации криптографических генераторов, основанных на усложнении регистров сдвига с ли-

нейной обратной связью. В модуле реализованы функции:

- EstimationMuY– оценивание распределения вероятностей $(r+1)$-грамм по реализации искаженной цепи Маркова (использует CalculationNu) [7];
- EstimationQ_Y – оценивание матрицы одношаговых переходов Q (EstimationQ_X) [7];
- EstimationH_Y – оценивание условной энтропии;
- AlgorithmA1Y - оценивание шаблона связей с помощью полного перебора (EstimationH_Y);
- AlgorithmA2Y – оценивание шаблона связей с помощью наращивания начального заданного шаблона;
- CalculationBIC_Y – вычисление байесовского информационного критерия (EstimationMuY);
- EstimationSR_Y – оценивание порядка и числа связей (AlgorithmA1Y, AlgorithmA2Y, CalculationBIC_Y);
- EstimationP – оценивание параметра искажения (EstimationMuX) [7].

3 ПРИМЕНЕНИЕ

Разработанная библиотека функций использовалась для оценки качества регистра сдвига с переменной обратной связью [3, 4], генератора Geffe [1, 8], SG-генсратора [1, 9], выходной последовательности germany.bit физического генератора из библиотеки Дж. Марсальи [10].

С помощью модуля цепей Маркова с частичными связями удалось [6, 11]:

- Осуществить с высокой точность поиск характеристических многочленов регистра сдвига с переменной обратной связью. Для заданных параметров генератора, обеспечивающих период выходной последовательности не менее, чем 2^{19}-1, используя 320 бит из 1000 случаев в 981 характеристические многочлены определены верно. Заметим, что использование теории полносвязных цепей Маркова потребовало выходных бит в 2^{24} раза больше.
- Показать сильное отклонение выходных последовательностей SG-генератора от «чисто» случайной последовательности. При выходной последовательности длины 2^{16} бит из 10000 реализаций количество отклоненных равнялось 5300 (в среднем должно быть 500) для параметров генератора, обеспечивающих период не менее, чем 2^{45}.
- Выявить зависимости в выходной последовательности физического генератора. Для заданных ограничениях на порядок и число связей, зависимость 120 порядка с 8 частичными связями наилучшим образом выявляет структуру исследуемой последовательности. Найденная зависимость может быть использована для построения характерного «портрета» физического генератора.

Использую модуль двоичных цепей Маркова с частичными связями при наличии аддитивных искажений удалось осуществить поиск параметров генератора Geffe по его выходной последовательность длины 2^{15} бит. Для параметров генератора, обеспечивающих период не менее, чем 2^{110}, из 100 случаев в 93 один из примитивных характеристических многочленов определялся верно. Зная данный характеристический многочлен можно восстановить модель этого генератора [12].

ЛИТЕРАТУРА

[1] Математические и компьютерные основы криптологии / Ю. С. Харин [и др.]. – Минск : Новое знание, 2003. – 382 с.

[2] Иванов, М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – М. : КУДИЦ-ОБРАЗ, 2003. 240 с.

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

[4] Максимов, Ю. И. О цепях Маркова, связанных с двоичными регистрами сдвига со случайными элементами / Ю. И. Максимов // Труды по дискретной математике. – 1997. – Т. 1. – С. 203-220.

[5] Blum, M. Independent unbiased coin flips from a correlated biased source - a finite state Markov chain / M. Blum // Combinatorica. – 1986. – Vol. 6, No. 2. – P. 97-108.

[6] Харин, Ю. С. Цепь Маркова s-го порядка с r частичными связями и статистические выводы о ее параметрах / Ю. С. Харин, А. И. Петлицкий // Дискретная математика. – 2007. – Т. 19, № 2. – С. 109-130.

[7] Петлицкий, А. И. Статистический анализ двоичной цепи Маркова с частичными связями при наличии аддитивных искажений / А. И. Петлицкий, Ю. С. Харин // Весці НАН Беларусі, Сер. фіз.-мат. навук. – 2008. – № 4. – С. 30-36.

[8] Geffe, P. How to protect data with ciphers that are really hard to break / P. Geffe // Electronics. – 1973. – Vol. 46, No. 1. – P. 99-101.

[9] Coppersmith, D. The shrinking generator / D. Coppersmith, H. Krawczyk, Y. Mansour // Lecture Notes In Computer Science. – 1994. – Vol. 773. – P. 22-39.

[10] Marsaglia, G. The Marsaglia random number CDROM with the Diehard battery of tests of randomness / G. Marsaglia // Florida State University [Electronic resource]. – 1995. – Mode of access: www.stat.fsu.edu/pub/diehard. – Date of access: 20.11.2008.

[11] Харин, Ю. С. Выявление зависимостей большой глубины на основе марковских моделей / Ю. С. Харин, А. И. Петлицкий, М. В. Мальцев // Штучний інтелект. – 2008. – № 3. – С. 121-127.

[12] Zeng, K. An improved linear syndrome algorithm in cryptanalysis with applications / K. Zeng, C. H. Yang, T. R. N. Rao // Lecture Notes In Computer Science. – 1991. – Vol. 537. – P. 34-47.