Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

5. Лидл Р., Нидеррайтер Г. Конечные поля: в 2 т.: пер. с англ. М.: Мир, 1988.
6. Липницкий В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. 2-е изд. Минск: БГУИР, 2006.

О СТОХАСТИЧЕСКОМ МОДЕЛИРОВАНИИ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ МАЛОПАРАМЕТРИЧЕСКИХ МОДЕЛЕЙ

М. В. МАЛЬЦЕВ, Ю. С. ХАРИН

НИИ прикладных проблем математики и информатики БГУ

Для надежного шифрования необходимы криптографические генераторы – программные, аппаратные или программно-аппаратные устройства, вырабатывающие последовательности случайных или псевдослучайных чисел [1, 2]. Выходные последовательности стойкого криптографического генератора должны быть неотличимы от равномерно распределенной случайной последовательности (РРСП) [1]. Элементы РРСП независимы в совокупности, но псевдослучайные последовательности вырабатываются генераторами по определенным детерминированным алгоритмам и в таких последовательностях присутствуют зависимости, как правило, большой глубины. Для описания таких зависимостей адекватной моделью является цепь Маркова порядка $s >> 1$ (ЦМ(s)) [3]. К сожалению, использовать ее на практике зачастую невозможно, поскольку число параметров D этой модели с N состояниями увеличивается экспоненциально с ростом s:

$$D = N^s(N–1).$$

В связи с этим необходимы так называемые малопараметрические (parsimonious) марковские модели, число параметров которых зависит от s полиномиально [4]. Примерами малопараметрических моделей являются MTD-модель Рафтери [5], цепь Маркова переменного порядка [6], цепь Маркова условного порядка [7]. Поскольку по мере развития криптографии усложняется структура разрабатываемых генераторов, то возникает потребность в построении новых математических моделей для их анализа. В данной работе представлены две новые модели, построенные на основе цепи Маркова s-го порядка с r частичными связями (ЦМ(s, r)) [8].

Первая модель, рассматриваемая в данной работе, – цепь Маркова с частичными связями с переменным шаблоном. Модель ЦМ(s, r), разработанная в Белорусском государственном университете, является вероятностной моделью регистра сдвига с линейной обратной связью. Для этой модели условное распределение вероятностей будущего состояния временного ряда зависит не от всех s предыдущих состояний, а лишь от r избранных, определяемых так называемым шаблоном связей. ЦМ(s, r) с переменным шаблоном описывает более сложные зависимости, при которых шаблон изменяется с течением времени. Подобная ситуация встречается в криптографических генераторах. К примеру, в прореживающем (self-shrinking) генераторе на каждом такте при выработке очередного бита выходной последовательности происходит выбор одного из двух полиномов обратной связи [9].

Приведем математическое описание ЦМ(s, r) с переменным шаблоном.

Примем обозначения: **N** – множество натуральных чисел; $A = \{0, 1,..., N-1\}$ – множество мощности $|A| = N \geq 2$;

$$J_n^m = (j_n, \ldots, j_m) \in A^{m-n+1},\ n, m \in \mathbf{N},\ n \leq m,$$ –

мультииндекс (последовательность индексов); $\{ x_t \in A : t \in \mathbf{N}\}$ – цепь Маркова порядка s с пространством состояний A и матрицей вероятностей одношаговых переходов $P = (p_{J_1^s, j_{s+1}}(t))$:

$$p_{J_1^s, j_{s+1}}(t) = \mathrm{P}\{x_t = j_{s+1} \mid X_{t-s}^{t-1} = J_1^s\},\ t = s+1, s+2,...,\ J_1^{s+1} \in A^{s+1};$$

$u \in \mathbf{N}$ – число шаблонов связи; $f(t) : \mathbf{N} \to \{1, \ldots, u\}$ – некоторая функция; $M(1),..., M(u)$ – u независимых шаблонов связей, представляющих собой целочисленные r-вектора с упорядоченными компонентами:

$$M^{(i)} = (m_1^{(i)}, \ldots, m_r^{(i)}), 1 = m_1^{(i)} < m_2^{(i)} < \ldots < m_r^{(i)} \leq s, i = 1, \ldots, u;$$

$Q^{(1)}, ..., Q^{(u)}$ – u независимых стохастических матриц размерности $r + 1$:

$$Q^{(i)} = (q^{(i)}_{J_1^r, j_{r+1}}),\ J_1^{r+1} \in A^{r+1},\ i = 1, \ldots, u.$$

Определение 1. Цепь Маркова x_t называется цепью Маркова s-го порядка с r частичными связями с переменным шаблоном, если ее вероятности одношаговых переходов имеют вид:

$$p_{J_1^s, J_{s+1}}(t) = q^{(\tau)}_{j_{m_1^{(\tau)}, \ldots, m_r^{(\tau)}}, j_{s+1}},\ J_1^{s+1} \in A^{s+1},\ \tau = f(t). \quad (1)$$

Формула (1) означает, что вероятность перехода $p_{J_1^s, J_{s+1}}(t)$ зависит не от всех s предыдущих состояний, а от r избранных, как и для модели ЦМ(s, r). Отличие обобщенной модели (1) состоит в том, что в каждый момент времени функция f определяет один из u шаблонов связей и соответствующую матрицу переходов, в зависимости от выбранного шаблона выбираются r из s последних состояний цепи Маркова, которые определяют элементы матрицы $Q^{(f(t))}$, используемые для генерирования будущего состояния. Число независимых параметров ЦМ(s, r) с переменным шаблоном при некоторой фиксированной функции f составляет:

$$D1 = u(Nr(N-1) + r - 1)).$$

В таблице 1 представлено сравнение числа параметров двоичных ЦМ(s) и ЦМ(s, r) с переменным шаблоном при $u = 4$ для различных значений порядка s и числа связей r.

Таблица 1 – Сравнение числа параметров ЦМ(s) и ЦМ(s, r)

(s, r)	(8, 2)	(16, 4)	(32, 6)	(64, 8)	(128, 16)	(256, 16)
D	256	65536	$\approx 4{,}3 \cdot 10^9$	$\approx 1{,}8 \cdot 10^{19}$	$\approx 3{,}4 \cdot 10^{38}$	$\approx 1{,}2 \cdot 10^{77}$
D_1	20	76	276	1052	262204	262204

Вторая модель, рассматриваемая в работе, обобщает ЦМ(s, r) для векторной цепи Маркова. Она построена для обнаружения зависимостей между блоками данных

в выходных последовательностях криптографических генераторов. Представим ее математическое описание. Обозначим: $m \in \mathbf{N}$ – число, которое будем называть размерностью цепи Маркова; $B_i = (b_{i1},..., b_{im}) \in A^m$, $i \in \mathbf{N}$ – m-мерный целочисленный вектор; $\{ X_t = (x_{t1}, \ldots, x_{tm}) \in A^m : t \in \mathbf{N}\}$ – однородная векторная цепь Маркова порядка s (ВЦМ(s)) с пространством состояний A^m и матрицей вероятностей одношаговых переходов $P = (p_{(B_1,\ldots,B_s),\, B_{s+1}})$, $B_1, \ldots, B_{s+1} \in A^m$:

$$p_{(B_1,\ldots,B_s),\, B_{s+1}} = \mathrm{P}\{X_t = B_{s+1} \mid X_{t-1} = B_s,..., X_{t-s} = B_1\}, \; t = s+1, s+2,...; \qquad (2)$$

$Q = (q_{(i_1,...,i_r),I_{r+1}})$ – некоторая стохастическая $N^r \times N^m$ – матрица, $i_1, \ldots, i_r \in A$, $I_{r+1} \in A^m$;

$$M_r = \{(k_1, l_1), (k_2, l_2), \ldots, (k_r, l_r)\} \subseteq M_* = \{(k, l) : 1 \le k \le s, 1 \le l \le m\} -$$

шаблон-множество, представляющее собой упорядоченный в лексикографическом порядке набор $1 \le r \le sm$ различных значений пар индексов, причем $k_1 = 1$; $S_{M_r}(B_t,..., B_{t+s-1}) = (b_{t+k_1-1,l_1},..., b_{t+k_r-1,l_r})$, $t = 1, 2,...,$ – функция-селектор, которая в соответствии с шаблон-множеством M_r "вырезает" r компонент из множества ms компонент $\{b_{u,l} : t \le u \le t+s-1, 1 \le l \le m\}$.

Определение 2. Если вероятности одношаговых переходов (2) допускают следующее малопараметрическое представление:

$$p_{(B_1,\ldots,B_s),\, B_{s+1}} = q_{S_{M_r}(B_1,...,B_s),B_{s+1}} = q_{(b_{k_1,l_1},...,b_{k_r,lr}),B_{s+1}}, \; B_1, \ldots, B_{s+1} \in A^m, \qquad (3)$$

то такая цепь Маркова называется векторной цепью Маркова с r частичными связями (ВЦМ(s, r)).

Из формулы (3) следует, что условное распределение вероятностей состояния X_t временного ряда в момент времени t зависит не от всех ms компонент s прошлых состояний, а только от r избранных компонент, которые определяются шаблон-множеством M_r. Если $r = sm$, то $M_r = M_*$, и в этом случае приходим к полносвязной векторной цепи Маркова s-го порядка. Если $m = 1$, то ВЦМ(s, r) превращается в ЦМ(s, r). Число независимых параметров ВЦМ(s, r) определяется по формуле

$$D2 = Nr(Nm-1) + 2r - 1.$$

В таблице 2 представлено сравнение двоичных ВЦМ(s) и ВЦМ(s, r) при $m = 4$ для различных значений порядка s и числа связей r.

Таблица 2 – Сравнение числа параметров ВЦМ(s) и ВЦМ(s, r)

(s, r)	(1, 2)	(2, 4)	(4, 6)	(8, 8)	(16, 10)	(32, 16)
D	240	3840	983040	$\approx 6{,}4 \cdot 10^{10}$	$\approx 2{,}8 \cdot 10^{20}$	$\approx 5{,}1 \cdot 10^{39}$
D_2	63	247	971	3855	15379	983071

Список литературы

1. Криптология / Ю.С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.

2. Зубков, А.М. Датчики псевдослучайных чисел и их применения / А.М. Зубков // Московский университет и развитие криптографии в России: материалы конференции в МГУ. – М.: МЦНМО, 2003. – С. 200–206.

3. Дуб, Дж.Л. Вероятностные процессы / Дж. Л.Дуб. – М.: Издательство иностранной литературы, 1956. – 605 с.

4. Kharin Yu. Parsimonious models for high-order Markov chains and their statistical analysis / Yu. Kharin // VIII World Congress on Probability and Statistics. Publ. House of Koc. Univ.: Istanbul, 2012. – P. 168–169.

5. Raftery, A.E. A model for high-order Markov chains / A.E. Raftery // J. Royal Statistical Society. – 1985. – Vol. B-47, № 3. – P. 528–539.

6. Buhlmann, P. Variable length Markov chains / P. Buhlman, A. Wyner // The Annals of Statistics. – 1999. – Vol. 27, № 2. – P. 480–513.

7. Мальцев, М.В. О тестировании выходных последовательностей криптографических генераторов на основе цепей Маркова условного порядка / М.В. Мальцев, Ю.С. Харин // Информатика. – 2013. – № 4. – С. 104–111.

8. Харин, Ю.С. Цепь Маркова с частичными связями ЦМ(*s*, *r*) и статистические выводы о ее параметрах / Ю.С. Харин, А.И. Петлицкий // Дискретная математика. – 2007. – Т. 19, № 2. – С. 109–130.

9. Meier, W. The self-shrinking generator / W. Meier, O. Sta□elbach // Advances in Cryptology, Euro crypt-94. – 1995. – Vol. 950. – P. 205–214.

ШИФРОВАНИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКОЙ ДИНАМИКИ

А.В. СИДОРЕНКО

Белорусский государственный университет

Широкое распространение информационных технологий и Интернета вызывают проблемы обеспечения безопасного хранения и передачи данных в виде изображений. Одним из наиболее эффективных способов для решения этой задачи является шифрование информации. Стандартные методы шифрования, включая AES, DES или RSA, из-за особенностей, свойственных изображениям, для этого практически не дают эффекта.

В последние годы появилось ряд алгоритмов шифрования изображений, использующих для маскирования динамический хаос. Благодаря присущим динамическому хаосу особенностям, связанным с наличием чувствительности к начальным условиям и случайности, такие методы подходят для шифрования изображений с высокой степенью защиты. При этом шифрование, как правило, происходит с использованием перестановки и диффузии. При перестановке с помощью хаотического отображения производится перераспределение пикселей изображения без изменения уровня их яркости. На стадии диффузии путем применения хаотической последовательности к изображению изменяется значение каждого пикселя.

В данной работе предлагается генетический алгоритм шифрования изображений с использованием модели дезоксирибонуклеиновой кислоты (ДНК) и динамического хаоса. В схеме предложенного нами алгоритма шифрования выделяются три этапа: инициализация, генерация изображений-шифров и использование генетического алгоритма. Два последних этапа могут повторяться до тех пор, пока не будут удовлетворять выбранным критериям. В нашем случае в качестве критерия используется достижение соответствующего уровня информационной энтропии в зашифрованном изображении, что обусловлено необходимостью обеспечения лучшего быстродействия функционирования алгоритма. Рассмотрим подробнее этапы алгоритма.