PolotskSU

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

PolotskSU

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

© Полоцкий государственный университет», 2017

PolotskSU

М-ва внутр. дел Респ. Беларусь»; редкол.: В. Б. Шабанов (отв. ред.) [и др.]. – Минск, 2015. С. 124–128.

4. Рыбальский О.В., Соловьев В.И., Железняк В.К. Спектральный анализ и современные речевые технологии. // Вестник Полоцкого государственного университета. Серия С. – 2014. – №4. – С. 2-6.

ЭНТРОПИЙНЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В.Ю. ПАЛУХА, Ю.С. ХАРИН

НИИ прикладных проблем математики и информатики БГУ

Введение. Важным структурным элементом средств криптографической защиты информации (криптосистем) являются генераторы случайных и псевдослучайных последовательностей [1]. Стойкость криптосистем зависит от того, насколько близка генерируемая последовательность по своим свойствам к равномерно распределённой случайной последовательности (РРСП).

Для проверки качества криптографических генераторов используются статистические тесты, суть которых заключается в следующем. Наблюдается выходная последовательность криптографического генератора и вводится гипотеза H_* о том, что последовательность является РРСП. Вычисляется некоторая статистика, распределение вероятностей которой при истинной гипотезе H_* известно. На основании значения статистики гипотеза H_* принимается либо отклоняется. В данном докладе рассматривается применение статистической оценки энтропии Шеннона в качестве тестовой статистики для анализа выходных последовательностей криптографических генераторов.

Математическая модель. Пусть на вероятностном пространстве (Ω, F, P) с множеством состояний $\Omega = \{\omega_1, \ldots, \omega_N\}$ определена случайная величина $x = x(\omega) = \omega$ с дискретным распределением вероятностей $P = \{p_k\},\ p_k = P\{x = \omega_k\},\ p_k \geq 0,\ \sum_{k=1}^{N} p_k = 1,\ k = 1, \ldots, N$. Энтропия Шеннона определяется формулой [1]

$$H(P) = -\sum_{k=1}^{N} p_k \ln p_k. \tag{1}$$

Пусть имеется случайная последовательность $\{x_t : t = 1, \ldots, n\}$ объёма n из распределения вероятностей $\{p_k\}$. Построим частотные оценки распределения вероятностей $\{p_k: k = 1, \ldots, N\}$:

$$\hat{p}_k = \frac{v_k}{n}, \quad v_k = \sum_{t=1}^{n} I\{x_t = \omega_k\} \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}, \quad I\{x_t = \omega_k\} = \begin{cases} 1, & x_t = \omega_k; \\ 0, & x_t \neq \omega_k. \end{cases} \tag{2}$$

Как уже было сказано во введении, введём в рассмотрение гипотезу $H_* = \{\{x_t\}$ является РРСП$\} = \{\{x_t\}$ – н.о.р.с.в., $p_k = 1/N$, $k = 1, \ldots, N\}$ и альтернативу $\overline{H_*}$.

Следуя [2], будем полагать, что имеет место схема серий. В таком случае вектор $(v_1, \ldots, v_N)^T$, составленный из частот v_k из (2), имеет полиномиальное распределение вероятностей $\mathrm{Pol}(n, N, p_1, \ldots, p_N)$, а каждая из компонент распределена по биномиальному

PolotskSU

закону $Bi(n, p_k)$. Рассмотрим асимптотику, в которой длительность наблюдения n и число значений N растут синхронно:

$$n, N \to \infty, n/N \to \lambda, 0 < \lambda < \infty, \tag{3}$$

В асимптотике (3) для распределения вероятностей статистик $\{\nu_k\}$ справедлива аппроксимация законом Пуассона $\Pi(\lambda_k)$ с параметром $\lambda_k = np_k$ [3]. При истинной гипотезе H_* все элементарные вероятности равны: $p_k = 1 / N$, $k = 1, \ldots, N$, поэтому все частоты $\{\nu_k\}$ имеют одинаковый параметр распределения Пуассона $\lambda = n / N$.

Статистическая оценка энтропии Шеннона $\hat{H}(n, N)$, построенная по подстановочному принципу с использованием частотных оценок вероятностей, записывается следующим образом:

$$\hat{H} = \hat{H}(n, N) = -\sum_{k=1}^{N} \hat{p}_k \ln \hat{p}_k = -\sum_{k=1}^{N} \frac{\nu_k}{n} \ln \frac{\nu_k}{n}. \tag{4}$$

Справедлива теорема, доказанная в [4], об асимптотическом распределении вероятностей статистики (4).

Теорема. В асимптотике (3) статистика (4) при истинной гипотезе H_* имеет асимптотически нормальное распределение $\mathcal{L}\left\{\frac{\hat{H} - \mu_H}{\sigma_H}\right\} \to \mathcal{N}_1(0,1)$:

$$\mu_H = \ln n - e^{-\lambda} \sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!}, \tag{5}$$

$$\sigma_H^2 = \frac{e^{-\lambda}}{n} \sum_{k=1}^{+\infty} \frac{(k+1)\lambda^k}{k!} \ln^2(k+1) - \frac{e^{-2\lambda}}{N} \left(\sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!} \right)^2 - \frac{e^{-2\lambda}}{n} \left(\sum_{k=1}^{+\infty} \ln(k+1) \frac{\lambda^k}{k!} (k+1-\lambda) \right)^2.$$

Знание асимптотического распределения точечной оценки (4) позволяет построить интервальную оценку энтропии Шеннона:

с вероятностью $1 - \varepsilon$ оценка энтропии $\hat{H}(P) \in (H_-, H_+)$, $H_\pm = \mu_H \pm \sigma_H \Phi^{-1}\left(1 - \frac{\varepsilon}{2}\right)$, (6)

где $\Phi(\cdot)$ – функция распределения стандартного нормального закона [3]. Решающее правило, основанное на интервальной оценке (6), имеет вид:

$$\begin{cases} H_*, & \text{если } t_- < \hat{H}(n, N) < t_+; \\ \overline{H_*}, & \text{в противном случае,} \end{cases} \quad t_\pm = \mu_H \pm \sigma_H \Phi^{-1}\left(1 - \frac{\varepsilon}{2}\right). \tag{7}$$

Энтропийный анализ двоичных последовательностей. Построенная точечная оценка (4) является смещённой, что продемонстрировано в [5]. В отличие от истинного значения энтропии Шеннона, которая при справедливости гипотезы H_* достигает своего максимального значения $\ln N$, значение статистической оценки энтропии Шеннона (4) наблюдаемой последовательности может быть как меньше, так и больше математического ожидания при справедливости гипотезы H_*, поскольку математическое ожидание (5) в асимптотике (3) не превышает максимальное возможное истинное значение энтропии: $\mu_H \le \ln N$. Поэтому решающее правило (7) является двусторонним. Основанием для отклонения гипотезы H_* может являться как малое, так и большое значение статистической оценки энтропии Шеннона.

Объясняется данный факт следующим образом. В асимптотике (3) число наблюдений, приходящихся на каждый элемент алфавита, конечно и относительно невелико, и для

PolotskSU

«чисто случайной» последовательности значения частот v_k могут отличаться между собой в некоторых допустимых пределах (более того, как будет объяснено далее, эти значения должны отличаться).

Большие колебания в значениях частот v_k приведут к тому, что значение статистики (4) будет меньше математического ожидания (5), а при приблизительно равных значениях частот v_k значение статистики (4) будет стремиться к максимуму и превысит математическое ожидание (5).

Однако равные значения частот v_k свидетельствуют об отсутствии случайности в наблюдаемых значениях, наличии зависимости и, возможно, даже периода. Примером такого генератора является регистр сдвига, в выходной последовательности которого поочерёдно встречаются все возможные значения s-грамм. Тест (7) позволяет идентифицировать такой генератор.

В проведённых компьютерных экспериментах двоичные последовательности «разрезались» на непересекающиеся подряд идущие фрагменты длины s (s-граммы): $X^{(t)} = (X_j^{(t)}) = (y_{(t-1)s+1}, \ldots, y_{ts}) \in \{0,1\}^s,\ \ t = 1, \ldots, n = [T/s]$.

Из полученных s-грамм формировалась новая последовательность $\{x_t\}$ из алфавита мощности $N = 2^s$ по правилу $x_t = \sum_{j=1}^{s} 2^{j-1} X_j^{(t)} + 1$. На рисунках представлены графики значений отклонений оценки энтропии Шеннона (4) от математического ожидания (5), делённых на границы доверительных интервалов: $\dfrac{\widehat{H} - \mu_H}{\sigma_H \Phi^{-1}(1-\varepsilon/2)}$, на уровне значимости $\varepsilon = 0.05$ в зависимости от s. На рисунке 1 представлен результат анализа последовательности длины $T = 500 \cdot 2^{23}$ физического генератора [6], на рисунке 2 представлен результат анализа последовательности длины $T = 2^{31}$ линейного регистра сдвига [1] с характеристическим многочленом 25-й степени.

Как видно из рисунка 1, значение оценки (4) у выходной последовательности генератора [6] при различных значениях s как превышает, так и не достигает математического ожидания (5), что характерно для РРСП; однако при некоторых s отклонение превышает допустимый порог и гипотеза H_* отклоняется. Из рисунка 2 видно, что гипотеза H_* отклоняется не только при $s > 25$, когда оценка энтропии (4) меньше ожидаемого значения (5) из-за того, что превышен порядок регистра, но и при $s \le 25$, поскольку в этом случае выходная последовательность является «слишком правильной» и значение оценки энтропии (4) превышает математическое ожидание (5).

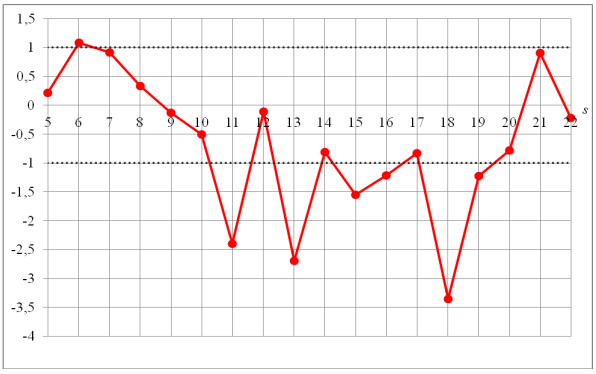

Рис. 1 – Нормированное отклонение оценки энтропии физического генератора

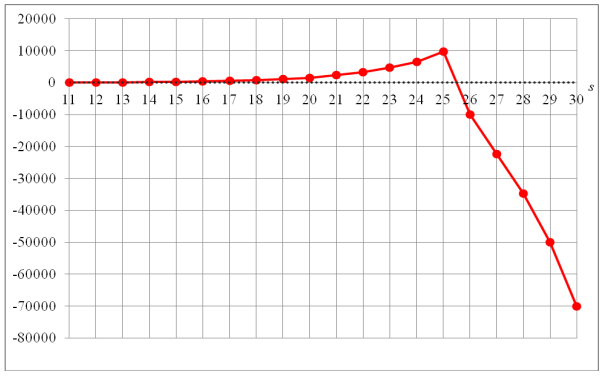

Рис. 2 – Нормированное отклонение оценки энтропии регистра сдвига

PolotskSU

Список литературы

1. Криптология / Ю. С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.
2. Holst, L. Asymptotic normality and efficiency for certain goodness-of-fit tests / L. Holst // Biometrika. – 1972. – №59. – P. 137–145.
3. Харин, Ю. С. Теория вероятностей, математическая и прикладная статистика / Ю. С. Харин, Н. М. Зуев, Е. Е. Жук. – Минск: БГУ, 2011. – 463 с.
4. Палуха, В. Ю. Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности / В. Ю. Палуха // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. – 2017. – № 1. – С. 79–88.
5. Палуха, В. Ю. Энтропийные характеристики двоичных последовательностей в криптографии / В. Ю. Палуха, Ю. С. Харин // Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19–21 мая 2015 г. – Минск: РИВШ, 2015. – С. 99–102.
6. Speedtest-500MB.bin [Electronic resource] // Humboldt Berlin University, Faculty of Mathematics and Natural Sciences, Department of Physics. – Mode of access: http://qrng.physik.hu-berlin.de/files/speedtest-500MB.bin. – Date of access: 08.04.2016.

ПРОГНОЗИРОВАНИЕ ДВОИЧНЫХ ВРЕМЕННЫХ РЯДОВ НА ОСНОВЕ МЕТОДА ИМИТАЦИИ ОТЖИГА

В.В. ПЬЯНОВ, Ю.С. ХАРИН

НИИ прикладных проблем математики и информатики 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 на основе метода имитации отжига.

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:

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