Выбор параметров и генерация секретов модулярного разделения осуществляется следующим образом. Сначала выбирается вспомогательный секрет $S(x) \in F_q[x]$ и модули (открытые ключи участников) $m_1(x), m_2(x), \ldots, m_k(x) \in F_q[x]$ и один дополнительный модуль (общий открытый ключ) $m(x)$. У всех многочленов $m_1(x), m_2(x), \ldots, m_k(x), m(x)$ должна быть одна и та же степень n. Хранимым секретом считается остаток от деления $S(x)$ на $m(x)$: $s(x) = S(x) \bmod m(x)$. Затем определяются частичные секреты (закрытые ключи участников) $s_i(x) = S(x) \bmod m_i(x), i = 1, \ldots, k$. Восстановление секрета $S(x)$ группой участников $1, 2, \ldots, l$, $l \leq k$, осуществляется путем решения соответствующей системы сравнений.

В работах [1], [2] предложен и изучался протокол верификации (t, k)-пороговой схемы, основанный на идее высказанной Бенало [3]:

1. Дилер генерирует случайный многочлен $S'(x)$, $\deg S'(x) < tn$.
2. Дилер сообщает каждому участнику значение $s'_i(x) = S'(x) \bmod m_i(x), i = 1, \ldots, k$.
3. Каждый участник публикует значение $p_i(x) = (s_i(x) + s'_i(x) \bmod m_i(x), i = 1, \ldots, k$.
4. Участники совместно находят $P(x)$ относительно $p_i(x)$, $i = 1, 2, \ldots, k$, $P(x) = S(x) + S'(x)$ и проверяют условие $\deg P(x) < tn$.

В работе [2] показано, что вероятность верификации при наличии лишь одного незаконного пользователя невелика. Например, в пороговом случае она равна $1/q^n$.

Нами обнаружено более сильное свойство предложенного протокола, основанное на следующей теореме.

Теорема. *Если в пороговой модулярной схеме в фазе восстановления секрета всеми участниками j частичных секретов, $1 \leq j \leq k - t$, окажутся ошибочными, то восстановленный секрет $S(x)$ будет неправильным, причем $deg\ S(x) \geq tn$.*

Эта теорема говорит о том, что предложенный протокол выявит наличии даже $j, 1 \leq j \leq k - t$, нарушителей, представивших неправильные частичные секреты, так как при его запуске не будет выполнено проверочное условие пункта 4: $\deg P(x) < tn$.

Литература

1. Васьковский М.М., Матвеев Г.В. *Верификация модулярного разделения секрета* // Журн. Бел. гос. ун-та Математика Информатика, 2, 2017, Минск. С.17–22.

2. Матвеев Г.В., Матулис В.В. *Совершенная верификация модулярной схемы* // Журн. Бел. гос. ун-та Математика Информатика, 2, 2018, Минск.

3. Benaloh J. *Secret sharing homomorphisms: keeping shares of a secret* // LNCS – 1987 – Vol. 263. P. 251–260.

ЭНТРОПИЙНЫЕ ФУНКЦИОНАЛЫ И ЭНТРОПИЙНЫЕ ПРОФИЛИ В ЗАДАЧАХ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

Палуха В.Ю., Харин Ю.С.

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220050 Минск, Беларусь {palukha, kharin}@bsu.by

Для проверки качества криптографических генераторов используются статистические тесты, в которых провеяется гипотеза $H_* = \{\{x_t\}$ является РРСП$\}$ о том, что наблюдаемая последовательность является равномерно распределённой случайной последовательностью. В качестве тестовой статистики могут выступать статистические оценки энтропии.

Пусть наблюдается n фрагментов длины s, сформированных из элементов двоичной последовательности $\{x_t\} \in V = \{0,\ 1\} : X^{(k)} = (x_1^{(k)},\ \ldots,\ x_s^{(k)}) \in V_s,\ k = 1,\ \ldots,\ n$. Обозначим: $x^{\underline{r}} = x(x-1)\ldots(x-r+1)$ – нисходящая факториальная степень; $p_J(s) = P\{X^{(k)} = J_1^s\}$,

$J_1^s = (j_1, \ldots, j_s) \in V_s$ – s-мерное распределение вероятностей. Построим оценки вероятностей $\{\widehat{p_J}\}$ и их r-ых степеней $\{\widehat{p_J^r}\}$, используя частотные статистики:

$$\widehat{p_J^r}(s) = \frac{v_J^r}{n^r}, \quad v_J = \sum_{k=1}^{n} \delta_{X^{(k)},J}, \quad \delta_{X^{(k)},J} = \begin{cases} 1, & X^{(k)} = J; \\ 0, & X^{(k)} \neq J, \end{cases}$$

и на их основе построим статистические оценки энтропии Шеннона $\widehat{H}(n,s) = -\sum\limits_{J \in V_s} \dfrac{v_J}{n} \ln \dfrac{v_J}{n}$, Реньи $\widehat{H_r}(n,s) = \dfrac{1}{1-r} \ln \left(\sum\limits_{J \in V_s} \widehat{p_J^r}(s) \right)$ и Тсаллиса $\widehat{S_r}(n,s) = \dfrac{1}{r-1} \left(1 - \sum\limits_{J \in V_s} \widehat{p_J^r}(s) \right)$, $r \in \mathbb{N}$, $r > 1$, которые в асимптотике n, $N = 2^s \to \infty$, $n/N \to \lambda$, $0 < \lambda < \infty$ имеют асимптотически нормальное распределение при гипотезе H_* [1].

Зададим уровень значимости $\alpha \in (0,\ 1)$. Введём обозначения: $\widehat{h(s)}$ – статистическая оценка энтропии Шеннона, Реньи или Тсаллиса, $\mu_h(s)$ – асимптотическое математическое ожидание, $\sigma_h^2(s)$ – асимптотическая дисперсия оценки при истинной гипотезе H_*, $\Phi^{-1}(\cdot)$ – квантиль стандартного нормального закона. Вычислим для наблюдаемой последовательности статистику $\widehat{h(s)}$. Решающее правило, основанное на статистике $\widehat{h(s)}$, имеет вид:

$$\text{принимается} \begin{cases} H_*, & \text{если } t_- < \widehat{h(s)} < t_+; \\ \overline{H_*}, & \text{в противном случае} \end{cases} \qquad t_\pm = \mu_h(s) \pm \sigma_h(s) \Phi^{-1}\left(1 - \frac{\alpha}{2}\right). \tag{1}$$

На основе решающего правила (1) мы можем вычислить последовательность нормированных отклонений оценки энтропии от математического ожидания в зависимости от s, т.е. последовательность величин

$$\chi(s) = \frac{\widehat{h(s)} - \mu_h}{\sigma_h(s)\Phi^{-1}(1-\alpha/2)}, \quad s = 1, \ldots, s_+,$$

которую будем называть энтропийным профилем. Тестирование с помощью профиля позволяет выносить решение о принятии или отклонении гипотезы H_* на основе решающего правила (1) по последовательности значений $\chi(s)$ для различных s; такое решение видится более аргументированным, чем при принятии его по результатам однократного применения теста (1) для одного значения s.

Литература

1. Палуха В.Ю. *Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности* // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. 2017. № 1. С. 79–88.

ТЕСТИРОВАНИЕ ИСТОЧНИКОВ СЛУЧАЙНОСТИ НА ОСНОВЕ ОЦЕНОК МИНИМАЛЬНОЙ ЭНТРОПИИ

Пирштук И.К.

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220030 Минск, Беларусь, pirshtuk@bsu.by

Введение. Постановка задачи. Случайные числа (СЧ) широко применяются в криптографических приложениях для формирования криптографических ключей, синхропосылок и других объектов с целью передачи зашифрованных данных. СЧ могут быть получены различными способами, чаще всего для генерации СЧ используются генераторы случайных чисел (ГСЧ). Рекомендуется использовать физические ГСЧ (ФСЧП). Требования к выходным