$$\begin{cases} \widetilde{s} \cdot M_{s-1} < p < m_0 M_{s-1}, \\ \widetilde{s} = \lceil n/2 \rceil + \lfloor n/30 \rfloor + (1 - |n|_2) \cdot \mathrm{sn}(-|n/2|_{15}) + |n|_2 \cdot \mathrm{sn}(7 - \lfloor n/2 \rfloor_{15}) < s, \end{cases}$$

то двухкаскадная композиционная конфигурация модулярной интерпретации сообщений в криптосистеме RSA с модулем p, базирующаяся на схеме (9), корректна, т. е. является реализуемой.

Алгоритмы кодирования и декодирования сообщений, основанные на модулярной интерпретации данных в СЗИ, отличаются простотой и высоким быстродействием. Это обусловлено тем, что их реализация практически требует лишь логических операций и операций присвоения. Для традиционно применяемых кодирующих и декодирующих процедур, основанных на позиционной интерпретации сообщений, необходимые временные затраты составляют величину порядка O(sn) модульных операций.

Список использованных источников

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. – М.: Физматлит, 2012. – 280 с.

2. Умножение и возведение в степень по большим модулям с использованием минимально избыточной модулярной арифметики [Текст] / А. Н. Каленик [и др.] // Информационные технологии. – 2012. – № 4. – С. 37–44.

3. Таблично-сумматорная алгоритмизация минимально избыточной модулярной схемы Монтгомери для умножения по большим модулям / А. А. Коляда [и др.] // Наука и военная безопасность. – 2013. – № 3. – С. 40–45.

4. *Червяков, Н. И.* Реализация алгоритма Монтгомери в системе остаточных классов на базе эффективного алгоритма расширения системы оснований / Н. И. Червяков, М. А. Дерябин, И. Н. Лавриненко // Нейрокомпьютеры: разработка, применение. – 2014. – № 9. – С. 37–45.

5. *Wu, Tao.* Improved RNS Montgomery modular multiplication with residue recovery / Tao Wu, Shoguo Lee, Litian Leu // Proc. Int. Conf. on soft computing techniques and engeneering aplication advances in intelligent systems and computing. – 2014. – Vol. 250. – P. 233–245.

6. *Bigou, K.* RNS modular multiplication through reduced base extentions / K. Bigou, A. Tisserand // 25 Int. Conf. «Application specific systems, architectures and processors (ASSAP 2014)». – Zurich, Switzerland. – 18–20 june, 2014. – IEEE. – P. 57–62.

7. *Лавриненко, А. Н.* Округление чисел по модулю поля эллиптической кривой при выполнении криптографических преобразований в системе остаточных классов / А. Н. Лавриненко, Н. И. Червяков // Инфокоммуникационные технологии. – 2014. – Т. 12, № 2. – С. 4–7.

РАСПОЗНАВАНИЕ И КОРРЕКТИРОВКА ВКРАПЛЕНИЙ В СТЕГАНОГРАФИИ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ

Ю. С. ХАРИН, Е. В. ВЕЧЕРКО, В. А. ВОЛОШКО

Актуальными задачами стеганографической защиты информации являются задачи распознавания и корректировки вкраплений [1–8]. Распознавание вкраплений включает в себя задачи обнаружения вкраплений и статистического оценивания точек вкраплений [7] (моментов времени, в которых содержится сообщение). Задача обнаружения (выявления) факта вкраплений рассматривается в работах [3; 5; 6; 8]; при этом предполагается, что вероятностная модель контейнера полностью известна. Так, в [5; 6] построены статистические критерии проверки гипотез о наличии вкраплений для случая, когда моделью контейнера является бернуллиевская схема независимых испытаний, построен наиболее мощный критерий проверки гипотез о наличии вкраплений и статистические оценки доли вкраплений. В [4] построены и исследованы статистические оценки параметров модели вкраплений в двоичную цепь Маркова.

Математическая модель контейнеров и процесса вкрапления. Введем обозначения: $V = \{0,1\}$ – двоичный алфавит, V_t – пространство двоичных

t-мерных векторов, N – множество натуральных чисел, $I\{A\}$ – индикатор события A, $u_{t_1}^{t_2} = (u_{t_1},...,u_{t_2}) \in V_{t_2-t_1+1}$ $(t_1, t_2 \in \mathrm{N},\ t_1 \le t_2)$ – двоичная строка из $t_2 - t_1 + 1$ символов, $w(\cdot)$ – вес Хемминга, $L\{\xi\}$ – закон распределения вероятностей случайной величины ξ, $B(\theta)$ – закон распределения вероятностей Бернулли с параметром $\theta \in [0,1]$. Будем предполагать, что исходный контейнер для встраивания сообщения есть двоичная последовательность $x_1^T \in V_T$, $x_t \in V, t = 1,...,T$, длины T, являющаяся однородной стационарной двоичной цепью Маркова 1-го порядка с симметричной матрицей вероятностей одношаговых переходов [4]:

$$\mathrm{P}\{x_{t+1} \oplus x_t = 1\} = \frac{1}{2}(1-\varepsilon),\ \ |\varepsilon| < 1. \tag{1}$$

Отметим, что цепь Маркова (1) удовлетворяет условиям эргодичности и имеет равномерное стационарное распределение вероятностей $\pi = (1/2, 1/2)$. Представленная модель контейнера (1) обоснована в [4] и достаточно хорошо согласуется с реальными статистическими данными.

Далее полагаем, что сообщение $\xi_1^M \in V_M$, $M \le T$, является последовательностью M независимых случайных величин Бернулли: $L\{\xi_t\} = B(\theta_1)$, $\mathrm{P}\{\xi_t = j\} = \theta_j$, $j \in V$, $\theta_1 = 1 - \theta_0$, $t = 1,...,M$. Как правило, $\{\xi_t\}$ имеет симметричное распределение: $\theta_1 = \theta_0 = 1/2$.

Стегоключ $\gamma_1^T \in V_T$ определяет моменты времени, в которые биты сообщения ξ_1^M вкрапляются в последовательность x_1^T. Введем специальную (q,r)-блочную модель стегоключа $(q, r \in \mathrm{N},\ r \le q)$, предполагая, что длина последовательности x_1^T кратна q: $T = Kq$. Для этого вначале разобьем последовательность x_1^T на блоки длины q: $x_{(1)} = x_1^q, x_{(2)} = x_{q+1}^{2q},..., x_{(K)} = x_{T-q+1}^T$. Введем вспомогательные независимые случайные величины $\varsigma_k \in V$, $L\{\varsigma_k\} = B(\delta)$, $k = 1,...,K$, которые отвечают за выбор блоков $\{x_{(k)}\}$ для вкрапления сообщения: если $\varsigma_k = 1$, то в r случайно выбранных бит блока $\{x_{(k)}\}$ вкрапляются r бит сообщения; если $\varsigma_k = 0$, то вкрапление в блок $\{x_{(k)}\}$ не производится.

Случайная стегопоследовательность $Y_1^T \in V_T$ порождается следующим образом:

$$Y_t = \gamma_t \xi_{\tau_t} + (1 - \gamma_t) x_t. \tag{2}$$

Последовательности $\{x_t\}$, $\{\xi_t\}$, $\{\gamma_t\}$ предполагаются независимыми в совокупности.

Методы распознавания вкраплений. Большинство работ по обнаружению факта вкраплений основано на эмпирических характеристиках последовательностей, в которых для проверки гипотез о наличии вкраплений используются методы дискриминантного анализа. На примере модели вкраплений (2) построим статистические критерии проверки гипотез о наличии вкраплений.

Определим две статистические гипотезы:

$$H_0 : \{\delta = 0\},\ H_1 = \{\delta > 0\}. \tag{3}$$

Гипотеза H_0 означает, что вкрапления отсутствуют и стегопоследовательность y_1^T совпадает с последовательностью x_1^T. Альтернатива $H_1 = \overline{H}_0$ означает наличие

вкраплений некоторой неизвестной доли $\delta > 0$. Если справедлива гипотеза H_0, то вероятностную меру P будем обозначать P_0, в противном случае – P_δ.

Введем статистику «знакоперемен» (число серий): $B_T = 1 + \sum_{t=1}^{T-1} y_t \oplus y_{t-1}$. Доказано, что если имеет место модель вкраплений (2), то при $T \to \infty$ асимптотический размер критерия

$$\chi_{1\alpha}^{B+} = \{y_1^T : B_T \geq 1 + (T-1)(1-\varepsilon)/2 - t_\alpha \sqrt{(T-1)(1-\varepsilon^2)/2}\},\ \varepsilon > 0,$$

$$\chi_{1\alpha}^{B-} = \{y_1^T : B_T \leq 1 + (T-1)(1-\varepsilon)/2 + t_\alpha \sqrt{(T-1)(1-\varepsilon^2)/2}\},\ \varepsilon < 0$$

на основе статистики числа серий B_T совпадает с наперед заданным уровнем значимости $\alpha \in (0,1)$. Асимптотическое выражение мощности этого критерия при $q = r = 1$ и контигуальных альтернативах $\delta = \dfrac{\rho}{T^\beta} \to 0$, $\beta > 0$, имеет вид

$$W_1^{B+} = W_1^{B-} = \begin{cases} 1,\ 0 < \beta < 1/2, \\ \Phi(t_\alpha + 2\rho \dfrac{|\varepsilon|}{\sqrt{1-\varepsilon^2}}) \quad \beta = 1/2, \end{cases}$$

где $\Phi(\cdot)$ – функция распределения стандартного нормального закона, $\Phi(t_\alpha) = \alpha$.

Также для данной модели вкраплений построен статистический критерий проверки гипотез (3) на основе статистики $\psi_T > 0$ длин серий.

Рассмотрим теперь случай, когда параметр ε в (1) неизвестен и отделен от нуля: $|\varepsilon| \leq \varepsilon_c$, где ε_c – известное граничное значение. Для проверки гипотез (3) о наличии и отсутствии вкраплений построим статистический критерий отношения правдоподобия. Статистика λ_T этого критерия имеет вид:

$$\lambda_T = 2(\ln \max(\ln L(\hat{\varepsilon}_1, \hat{\delta}_1), \ln L(\hat{\varepsilon}_0, 0) - \ln L(\hat{\varepsilon}_0, 0)) \geq 0,$$

где L – функция правдоподобия для (q,r)-блочной модели вкраплений (1), $\hat{\varepsilon}_0, \hat{\varepsilon}_1, \hat{\delta}_1$ – МП-оценки, построенные в [4], соответственно при условии H_0, H_1. Статистический критерий размера $\alpha \in (0,1)$ на основе статистики λ_T задается критической областью $\chi_{1\alpha}^{\lambda} = \{y_1^T \in V_T : \lambda_T \geq \lambda_\alpha\}$. Если выполняются достаточно общие условия регулярности, то для вычисления порога λ_α можно использовать известные асимптотические свойства критерия отношения правдоподобия.

Методы корректировки вкраплений. Под стеганографической емкостью будем понимать максимальную пропускную способность среди стегосистем из некоторого параметризованного класса. При этом можно говорить о емкости контейнера относительно некоторого класса алгоритмов встраивания и последующей маскирующей корректировки. Если алгоритм статистический, как в настоящей работе, то емкость становится параметром вероятностной модели контейнера. В приведенном выше алгоритме встраивания контейнер x_t предполагается двоичной цепью Маркова первого порядка M(ε), -1<ε<+1, с симметричной матрицей переходных вероятностей и вероятностью смены состояния (1-ε)/2. Выбирающий процесс (селектор) γ_t, определяющий точки вкрапления, предполагается схемой независимых испытаний B(δ) с долей единиц 0<δ<1. Последняя играет роль пропускной способности. Встраиваемое сообщение предполагается белым шумом B(1/2). Теперь для маскирующей корректировки поставим своей целью сгенерировать псевдослучайный стационарный процесс-корректор, не зависящий от трех исходных процессов, участвующих во встраивании. Корректор

должен быть таким, чтобы замена бит контейнера соответствующими битами корректора в тех позициях, которые не заняты сообщением, приводила к восстановлению вероятностей и частот встречаемости каждого двоичного слова вплоть до некоторой заданной длины n. Оказывается, в таких условиях распределение вероятностей слов длины n корректора однозначно определено и существует при $\delta<\delta_n$, где δ_n будем называть простой n-емкостью контейнера (почему простой – объяснено ниже). В качестве корректора подойдет любой стационарный эргодический процесс с таким распределением слов длины n, например, цепь Маркова порядка n с этим распределением, взятым в качестве ее стационарного распределения. Очевидно, последовательность простых n-емкостей не возрастает: $\delta_1 \ge \delta_2 \ge \ldots$. Для рассмотренного марковского контейнера M(ε) найдены точные значения простых 2-, 3- и 4-емкостей, а также получена предполагаемая асимптотика простой n-емкости при больших n:

$$\delta_2 = 1-\sqrt{|\varepsilon|}, \quad \delta_3 = 1-\sqrt{|\varepsilon|(2-|\varepsilon|)}, \quad \delta_4 = 1-\sqrt{\kappa+\kappa^2-\kappa^3},$$

$$\delta_n = \Delta_0 + \frac{\Delta_2}{n^2} + \frac{\Delta_3}{n^3} + \frac{\Delta_4}{n^4} + O\left(\frac{1}{n^5}\right),$$

где $\kappa = (1-|\varepsilon|+\sqrt{5+\varepsilon^2-2|\varepsilon|})/2$, $\Delta_0 = 1-\mu$, $\Delta_2 = \mu(1-\mu^2)\pi^2/2$, $\Delta_3 = -\mu(1-\mu^2)^{3/2}\pi^2$,

$$\Delta_4 = \frac{\mu(1-\mu^2)(36-\pi^2+(9\pi^2-36)\mu^2)}{24}\pi^2, \ \mu = \frac{2\sqrt{|\varepsilon|}}{1+|\varepsilon|}.$$

Стоит отметить существование нетривиального предела $\delta_\infty = \Delta_0$ простых n-емкостей цепи Маркова M(ε) с ростом n.

В литературе, как правило, моменты встраивания полагаются независимыми между собой. Если же селектор не предполагать схемой независимых испытаний, а требовать от него лишь стационарности и эргодичности, можно достичь увеличения емкости и, соответственно, пропускной способности. В таких условиях корректор, если он существует, снова однозначно определен с точностью до вероятностей слов длины n. Эти вероятности могут быть вычислены по соответствующим вероятностям контейнера и селектора. Максимальную пропускную способность δ_n^*, обеспечивающую существование корректора в условиях произвольного селектора, будем называть абсолютной n-емкостью (в отличие от простой n-емкости, максимизирующей пропускную способность в условиях бернуллиевского селектора). Для марковского контейнера M(ε) абсолютные 2- и 3-емкости имеют вид

$$\delta_2^* = 1-|\varepsilon|, \quad \delta_3^* = (1-|\varepsilon|)^2.$$

Графики найденных емкостей приведены на рис. 1. По оси абсцисс отложена вероятность смены состояния (1-ε)/2.

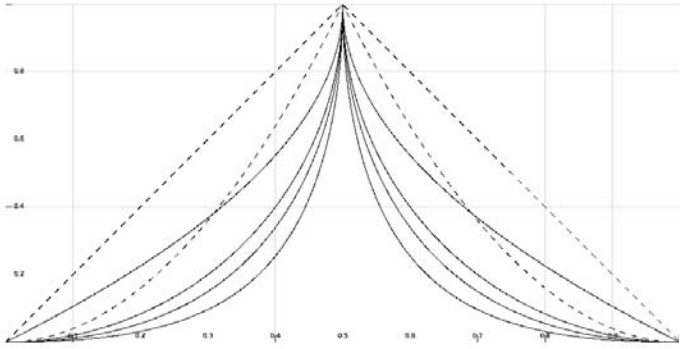

Рис. 1. **Емкости цепи Маркова M(ε): пунктир –** $\delta_2^* > \delta_3^*$**, сплошные –** $\delta_2 > \delta_3 > \delta_4 > \delta_\infty$

Список использованных источников

1. *Wang Y., Moulin P.,* «Perfectly Secure Steganography: Capacity, Error Exponents, and Code Constructions», IEEE Transactions on Information Forensics and Security, 54:6 (2008), 2706–2722.
2. *Harmsen J. J., Pearlman W. A.,* «Capacity of Steganographic Channels», IEEE Transactions on Information Theory, 55 (2009), 1775–1792.
3. *Filler T., Ker A. D., Fridrich J.,* «The Square Root Law of Steganographic Capacity for Markov Covers», Media Forensics and Security XI. Volume 7254 of Proc. SPIE, San Jose, 2009, 0801–0811.
4. *Харин Ю. С., Вечерко Е. В.* «Статистическое оценивание модели вкраплений в двоичную цепь Маркова», Дискретная математика, 25:2 (2013), 135–148.
5. *Пономарев К. И.,* «Параметрическая модель вкрапления и ее статистический анализ», Дискретная математика, 21:4 (2009), 148–157.
6. *Пономарев К. И.,* «Об одной статистической модели стеганографии», Дискретная математика, 21:2 (2009), 138–145.
7. *Харин, Ю. С., Вечерко, Е. В.* «Распознавание вкраплений в марковскую последовательность», Вопросы защиты информации, 107:4 (2014), 73-76.
8. *Ker A.,* «A capacity result for batch steganography», IEEE Signal Processing Letters, 14:8 (2007), 525–528

ПРИНЦИПЫ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ ПРОГРАММНЫХ БИБЛИОТЕК: БИБЛИОТЕКА BEE2

С. В. АГИЕВИЧ

Криптографические программные библиотеки должны не только точно и эффективно реализовывать криптографические алгоритмы и протоколы, но и соответствовать дополнительным принципам безопасности. В докладе рассматриваются принципы построения библиотеки Bee2, разработанной автором. На сегодняшний день в библиотеке реализованы алгоритмы и протоколы национальных криптографических стандартов (СТБ 34.101.31, 45, 47, 60, 66), а также алгоритмы электронной цифровой подписи, стандартизированные в Российской Федерации и Украине.

Переносимость. Библиотека написана на языке Си, без ассемблерных вставок и поэтому компилируется практически на любой аппаратно-программной платформе с помощью средств GCC. Расширения C99 не использованы, поэтому библиотека компилируется также в среде Visual Studio любой версии.

Контроль памяти. В низкоуровневые функции библиотеки могут передаваться указатели state и stack. Эти указатели ссылаются на память, в которой размещаются состояния алгоритмов/протоколов и могут размещаться локальные переменные. Память может содержать критические объекты (ключи), и поэтому взята под контроль. Функции объявляют о потребностях в памяти через дополнительные сервисные функции (они имеют суффиксы keep и deep). Высокоуровневые функции обрабатывают объявления и определяют общий объем памяти для состояния и стека. Интересно, что объем памяти оказывается довольно небольшим. Так, в текущей реализации достаточно сложного протокола BMQV, определенного в СТБ 34.101.66, на максимальном уровне стойкости $l = 256$ каждой стороне требуется не более 4096 байтов (одной страницы) памяти.

Защита памяти. Динамическая память выделяется только в высокоуровневых функциях и только одним блоком: в нем размещаются и состояние, и стек всех подчиненных функций. Максимальный отказ от динамической памяти снижает риск типичных для языка Си ошибок, повышает контроль над критическими данными. В определенных операционных системах блок памяти может защищаться от попадания в файл подкачки. При завершении работы с блоком его очистка выполняется так, что не может показаться бесполезной оптимизатору, и он ее не исключит из кода библиотеки.

Регуляризация. Если в криптографических программах имеются условные переходы, и условия переходов определяются обрабатываемыми данными (но не их раз-