УДК 681.327.8:519.81
В.К. Маригодов, В.Л. Хайков
Севастопольский национальный технический университет
Студгородок, г. Севастополь, Украина, 99053
E-mail: root@sevgtu.sebastopol.ua

ЭНТРОПИЙНАЯ ОЦЕНКА СОВЕРШЕННОЙ СТОЙКОСТИ ШИФРА С ПОЗИЦИЙ ТЕОРИИ ИГР

В условиях конфликтной ситуации взаимодействия шифровальщика и криптоаналитика (дешифровальщика) найдены минимаксные рандомизированные стратегии упомянутых сторон и цена игры.

Введение. В настоящее время в результате разработки и практического использования новых методов криптоанализа, а также значительного повышения производительности вычислительных средств появилась реальная возможность раскрытия таких шифров, которые ранее считались совершенно стойкими [1].

Совершенно стойким по Шеннону шифром называется шифр, для которого выполнено равенство

$$p(y/x) = p(y),\ \forall y \in Y,\ \forall x \in X, \tag{1}$$

где x – открытый текст; y – шифрованный текст; Y, X – множества открытых и шифрованных текстов шифра, соответственно; $p(y)$ – распределение вероятности шифрованного текста; $p(y/x)$ – условное распределение вероятности шифрованного текста при известном открытом тексте.

Энтропийная оценка совершенной стойкости шифра имеет следующий вид:

$$H(X/Y) = H(X). \tag{2}$$

В формуле (2) $H(X)$ – энтропия непустого конечного множества открытых текстов; $H(X/Y)$ – условная энтропия непустого конечного множества открытых текстов при известном шифрованном тексте. Равенство (2) выполняется лишь в случае статистической независимости X и Y.

Теоретико-игровая оценка стойкости шифра [1,2], а также в других, известных авторам работах, не исследовались, т.е. в таком аспекте игровая постановка задачи является приоритетной.

Пусть в конфликтной ситуации взаимодействия оператор системы передачи информации (СПИ), т.е. игрок 1 (шифровальщик), стремится максимизировать дифференциальную энтропию

$$H_X(p) = -\sum_{i=1}^{n} p_i \ln(p_i) \tag{3}$$

выбором в качестве своей стратегии $p_i = F(x_i)$, $i = \overline{1,n}$. Стратегия игрока 2 (криптоаналитика) состоит в выборе $q_j = F(y_j)$, $j = \overline{1,m}$ или дифференциальной энтропии

$$H_Y(q) = -\sum_{j=1}^{m} q_j \ln(q_j) \tag{4}$$

такой, чтобы минимизировать (3). Однако при этом криптоаналитик лишь располагает возможностью минимизировать совместную дифференциальную энтропию

$$H_{X,Y} = -\sum_{i=1}^{n}\sum_{j=1}^{m} F(x_i)F(y_j/x_i)\ln\left[F(x_i)F(y_j/x_i)\right] \tag{5}$$

или условную дифференциальную энтропию

$$H_{Y/X} = -\sum_{i=1}^{n}\sum_{j=1}^{m} F(y_j/x_i)\ln\left[F(y_j/x_i)\right]. \tag{6}$$

1. Определение средних выигрышей сторон. Рассмотрим бескоалиционную биматричную игру и найдем ситуации равновесия, а также средние выигрыши сторон (минимаксные значения дифференциальных энтропий $H_x(p)$ и $H_{y/x}(q)$). Выигрыши оператора СПИ (шифровальщика) и криптоаналитика задаются соответственно матрицами:

$$H_1 = \left(h_{1ij}\right) = \begin{pmatrix} h_{111} & .. & h_{11j} & .. & h_{11n} \\ .. & .. & .. & .. & .. \\ h_{1i1} & .. & h_{1ij} & .. & h_{1in} \\ .. & .. & .. & .. & .. \\ h_{1m1} & .. & h_{1mj} & .. & h_{1mn} \end{pmatrix}, \tag{7}$$

$$H_2 = \left(h_{2ij}\right) = \begin{pmatrix} h_{211} & .. & h_{21j} & .. & h_{21n} \\ .. & .. & .. & .. & .. \\ h_{2i1} & .. & h_{2ij} & .. & h_{2in} \\ .. & .. & .. & .. & .. \\ h_{2m1} & .. & h_{2mj} & .. & h_{2mn} \end{pmatrix}. \tag{8}$$

Здесь h_{1ij}, h_{2ij} – возможные чистые стратегии игроков (значения дифференциальных энтропий).

Пусть у игрока 1 имеется n чистых стратегий, а у игрока 2 имеется m чистых стратегий. Поскольку для всякой биматричной игры существует си-

туация равновесия в ее смешанном расширении, перейдем к смешанным (рандомизированным) стратегиям. Тогда $p = (p_1,...,p_n)$ – полный набор вероятностей своих чистых стратегий – рандомизированная стратегия 1 игрока; $q = (q_1,...,q_m)$ – такая же стратегия игрока 2.

Средние выигрыши игроков 1 и 2 соответственно равны:

$$\left.\begin{aligned} \overline{H}_1(H_1,p,q) &= -\sum_{i=1}^{n}\sum_{j=1}^{m} h_{1ij}\,p_i q_j \\ \overline{H}_2(H_2,p,q) &= -\sum_{i=1}^{n}\sum_{j=1}^{m} h_{2ij}\,p_i q_j \end{aligned}\right\}. \qquad (9)$$

Ситуация равновесия для такой игры составляет пару (p,q) таких рандомизированных стратегий игроков, которые удовлетворяют неравенствам:

$$\sum_{i=1}^{n} h_{1ij}\,p_i \le \sum_{i=1}^{n}\sum_{j=1}^{m} h_{1ij}\,p_i q_j, \quad i = \overline{1,n}\ , \qquad (10)$$

$$\sum_{j=1}^{m} h_{2ij}\,q_j \le \sum_{i=1}^{n}\sum_{j=1}^{m} h_{2ij}\,p_i q_j, \quad j = \overline{1,m}\ . \qquad (11)$$

Для определения ситуаций равновесия необходимо решить систему неравенств (10), (11) относительно неизвестных $p = (p_1,...,p_n)$, $q = (q_1,...,q_m)$ при естественных условиях нормировки

$$\sum_{i=1}^{n} p_i = 1\ ,\quad \sum_{j=1}^{m} q_j = 1\ ,\quad p_i \ge 0\ \ (i = \overline{1,n}),\ \ q_j \ge 0\ ,\ \ (j = \overline{1,m})\ .$$

Для упрощенного случая биматричной игры с матрицами выигрышей 2×2 множества решений игроков легко находятся [2].

Согласно игровому подходу для шифровальщика и криптоаналитика существуют оптимальные (минимаксные) рандомизированные стратегии соответственно $p^* = (p_1^*,...,p_n^*)$ и $q^* = (q_1^*,...,q_m^*)$ такие, что с их учетом получаем из (9)

$$\overline{H}_1^* = \overline{H}_1(h_1,p^*,q^*) = \min_q \max_p \overline{H}_1(h_1,p,q) = \max_p \min_q \overline{H}_1(h_1,p,q)\ , \qquad (12)$$

$$\overline{H}_2^* = \overline{H}_2(h_2,p^*,q^*) = \min_q \max_p \overline{H}_2(h_2,p,q) = \max_p \min_q \overline{H}_2(h_2,p,q)\ . \qquad (13)$$

Для гауссовских распределений p^* и q^* цена игры, в качестве которой принята пропускная способность канала с общими медленными замираниями, найдена в [3].

2. Оптимальные стратегии и цена игры. Предположим, что шифровальщик (игрок 1) максимизирует энтропию (3) при дополнительных усло-

виях нормировки p_i и фиксации средней мощности шифруемого сигнала, т.е. при

$$\sum_{i=1}^{n} p_i = 1\,, \quad p_i \geq 0\,, \quad P = \sigma^2 = \sum_{i=1}^{n} x_i^2 p_i\,,$$

где σ^2 – дисперсия зашифрованного сигнала x_i.

Максимум энтропии при этих условиях реализуется для гауссовского распределения [4]

$$p_i(x)_{extr} = \frac{1}{\sqrt{2\pi\sigma^2}} \sum_{i=1}^{n} \exp\left(-\frac{x_i^2}{2\sigma^2}\right)\,. \tag{14}$$

Дифференциальная энтропия гауссовской случайной величины зависит только от ее дисперсии, т.е.

$$H_x(p) = \frac{1}{2}\left[\ln\left(2\pi\ e\sigma^2\right)\right]\log_2 e = \log_2\sqrt{2\pi\ e\sigma^2}\,.$$

Для нахождения экстремального распределения $p_j(y/x)_{extr}$ перепишем (5) в виде

$$H_{x,y}(p,q) = -\sum_{i=1}^{n}\sum_{j=1}^{m} \alpha\ \ q_j(y/x)\ln\left[\alpha\ \ q_j(y/x)\right], \tag{15}$$

где $\alpha = \frac{1}{\sqrt{2\pi\sigma^2}} \sum_{i=1}^{n} \exp\left(-\frac{x_i^2}{2\sigma^2}\right)$, и минимизируем функционал (15) при дополнительном условии, в качестве которого выбрана естественная нормировка $q_j(y/x)$, т.е.

$$\sum_{j=1}^{m} q_j(y/x) = 1\,, \quad q_j(y/x) \geq 0\,, \quad j = \overline{1,m}\,.$$

Вариационная техника и решение уравнения Эйлера-Лагранжа дают следующий результат

$$q_j(y/x)_{extr} = \exp\left[-\left(\alpha + \frac{\mu}{\alpha}\right)\right], \tag{16}$$

где μ – множитель неопределенности Лагранжа, который находится из приведенного выше условия нормировки.

Если ввести обозначение $\beta = \exp\left[-\left(\alpha + \frac{\mu}{\alpha}\right)\right]$, то параметры α и β представляют собой искомые минимаксные (оптимальные) стратегии игроков. Цена игры при этом определяется выражением

$$\overline{H}_1\left(h_1, p^*, q^*\right) = \overline{H}_2\left(h_2, p^*, q^*\right) = H^* = \overline{H}_1(\alpha,\beta) = \overline{H}_2(\alpha,\beta)\,. \tag{17}$$

Если принять $\alpha >> \mu$, то получим из (16) $q_j(y/x)_{extr} = \beta \approx \exp(-\alpha)$. С учетом этого при использовании (15) и (17) находим

$$\overline{H}_1(\alpha,\beta) = \alpha^2 \ln(\alpha)\exp(-\alpha) \quad . \tag{18}$$

На рисунке 1 изображена зависимость цены игры (18) от значения α. Из рисунка видно, что цена игры имеет максимальное значение при $\alpha = 3$.

Экспоненциальное распределение (16), а также экспоненциальный характер (18) обычно имеют место при передаче информации по каналам с общими медленными замираниями [4].

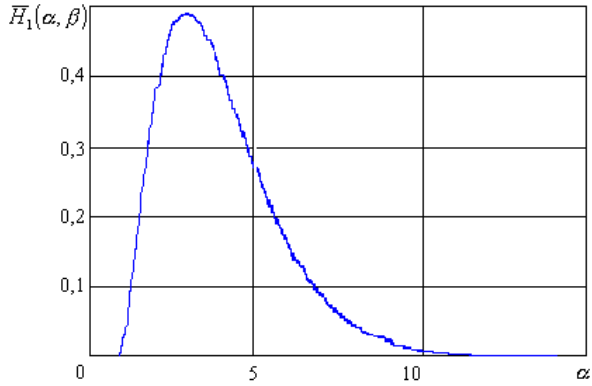

Рисунок 1 – Зависимость цены игры от параметра α

Заключение. Таким образом, найдены минимаксные стратегии шифровальщика и криптоаналитика, а также цена игры (среднее значение дифференциальной энтропии для рандомизированных стратегий сторон).

Задача обеспечения совершенной стойкости шифра оператором СПИ решается на основе соотношений (1) и (2). Выражения (4)-(18) позволяют определить *средние выигрыши игроков*, а также произвести энтропийную оценку рандомизированных минимаксных стратегий. Что касается *практической стойкости шифра*, то она определяется трудозатратами криптоаналитика на логические и вычислительные задачи для вскрытия ключей шифра и требует отдельного рассмотрения.

Перспективами дальнейших исследований в данном направлении могут стать следующие:

1) теоретико-игровая оценка практической стойкости шифра в системах телекоммуникации;
2) теоретико-игровая оценка помехоустойчивости шифра в различных ситуациях;
3) потенциальная оценка минимаксных затрат криптоаналитика.

Библиографический список

1. Банкет В.Л. Защита информации в системах телекоммуникации: Учеб. пособие / В.Л. Банкет, Н.В. Захарченко, А.В. Дырда; Под ред. В.Л. Банкета. — Одесса: Изд-во Укр. гос. акад. связи им. А.С.Попова, 1997. — 95 с.

2. Крушевский А.В.Теория игр / А.В. Крушевский. — К.: Выща шк., 1977. — 216 с.

3. Маригодов В.К. Оптимизация систем передачи информации в условиях активных помех / В.К. Маригодов // Отбор и перед. инф. — 1987. — Вып. 75. — С. 3–4.

4. Маригодов В.К. Помехоустойчивая обработка информации: Методы оптимального линейного предыскажения и корректирования / В.К. Маригодов. — М.: Наука, 1983. — 201 с.

Поступила в редакцию 7.03.2003 г.