ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 5
2016

Г. Б. Маршалко, **В. О. Миронкин** (Москва, ТК 26, МИЭМ НИУ ВШЭ)**. О свойствах одного нейросетевого алгоритма симметричного шифрования.**

В работах [1, 2] предложен симметричный алгоритм шифрования, основанный на использовании нейронных сетей. В этом алгоритме множество ключей K совпадает с множеством нейронных сетей, определенных на множестве A из m элементов, выходы которых принимают значение во множестве из $2^n \geqslant m$ элементов. Последнее неравенство означает, что одному символу открытого текста может соответствовать несколько различных шифрвеличин. Мощность множества шифрвеличин, соответствующих одному символу, пропорциональна вероятности его появление в тексте.

Каждая нейронная сеть $k \in K$ определяет правило зашифрования $E_k(a_i, w_i) : A \to V_n$, $i \in \{1, 2, \ldots, m\}$, следующим образом:

1) букве открытого текста $a_i \in A$, в соответствии с проведенной процедурой обучения сети, ставится в соответствие область Π_i;

2) на основе w_i (случайной величины, равномерно распределенной на множестве точек области Π_i) осуществляется случайный выбор точки области, которая и будет являться результатом шифрования буквы a_i.

Будем считать, что для исходного алфавита $A = \{a_1, a_2, \ldots, a_m\}$ определена вероятностная схема A [3]:

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \\ p(a_1) & p(a_2) & \cdots & p(a_m) \end{pmatrix}, \quad \sum_{i=1}^{m} p(a_i) = 1, \quad 0 < p(a_1) < 1,$$

где a_i — исход вероятностной схемы, $p(a_i)$ — вероятность этого исхода.

При помощи схемы A строится объединенная вероятностная схема на биграммах:

$$A^2 = \begin{pmatrix} a_1a_1 & a_1a_2 & \cdots & a_na_n \\ p(a_1a_1) & p(a_1a_2) & \cdots & p(a_na_n) \end{pmatrix}.$$

Пространство шифрвеличин разбивается на области $\Pi_1, \Pi_2, \ldots, \Pi_m$, каждая из которых задается своим центром $b_i^{(0)}$ и радиусом ε_i:

$$\Pi_i = \left\{ z \in V_n : \left\| b_i^{(0)} - z \right\| \leqslant \varepsilon_i \right\}, \qquad i \in \{1, 2, \ldots, m\},$$

где $\| \ \|$ — расстояние Хэмминга.

Распределение на множестве букв открытого текста, определяемое вероятностной схемой, индуцирует распределение на множестве областей Π_i, $i \in 1, 2, \ldots, m$, пространства шифрвеличин: $p(\Pi_i) = r_i/2^n$, где r_i — число элементов пространства шифрвеличин, лежащих в области Π_i.

Отметим, что для того чтобы рассматриваемый шифр был стойким относительно методов, использующих частотный анализ, мера каждой из областей Π_i должна совпадать с вероятностью соответствующей буквы a_i : $r_i/2^n = p(a_i)$, откуда следует, что значения ε_i однозначно определяются априорным распределением букв открытого сообщения:

$$\sum_{i=1}^{\varepsilon_i} \binom{n}{i} = p(a_i)2^n. \tag{1}$$

Пусть теперь $N(a_i)$, $i \in \{1,2,\ldots,m\}$, есть число вхождений символа a_i в открытом сообщении, а $N(a_ia_j)$, $i,j \in \{1,2,\ldots,m\}$, — число вхождений биграммы a_ia_j. При достаточно большом объеме $T \to \infty$ справедливы приближенные асимптотические равенства [5]:

$$\frac{N(a_i)}{T} \approx p(a_i) \quad \text{и} \quad \frac{N(a_ia_j)}{T-1} \approx p(a_ia_j). \tag{2}$$

Обозначим $\chi_{ij}^{(k,l)}$ расстояние между произвольными точками $b_i^{(k)}, b_j^{(l)}$ областей Π_i, Π_j в пространстве шифрвеличин: $\chi_{ij}^{(k,l)} = \|b_i^{(k)} + b_j^{(l)}\|$.

Так как согласно (1) все значения $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ определяются однозначно, для расстояний между центрами двух различных областей справедлива оценка снизу:

$$\chi_{ij}^{(0,0)} \geqslant 2\min\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m\}.$$

Для восстановления открытого текста на основе расстояний $\chi_{ij}^{(k,l)}$ будем использовать следующий алгоритм.

Алгоритм

1. С учетом имеющейся априорной информации о значениях $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ выбираем биграмму $b_i^{(k)}b_j^{(l)}$ в шифртексте с максимальным расстоянием

$$\chi_{ij}^{(k,l)} = \left\|b_i^{(k)} + b_j^{(l)}\right\| \geqslant 2\min\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m\}.$$

2. Обозначим $\delta \in [\min\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m\}; \max\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m\}]$ параметр, характеризующий погрешность определения точек областей Π_i, Π_j. Для полученного значения $\chi_{ij}^{(k,l)}$ находим все биграммы шифртекста, для которых расстояние Хэмминга принадлежит интервалу $\left[\chi_{ij}^{(k,l)} - 2\delta, \chi_{ij}^{(k,l)} + 2\delta\right]$.

3. Среди отобранных биграмм $b_i^{(u_1)}b_j^{(v_1)}, \ldots, b_i^{(u_d)}b_j^{(v_d)}$, $d \geqslant p(a_ia_j)T$, проведем отбраковку ложных вариантов. Оставим лишь те биграммы, для которых одновременно выполняются равенства

$$\left\|b_i^{(u_s)} + b_i^{(k)}\right\| \leqslant 2\delta, \quad \left\|b_j^{(v_s)} + b_j^{(l)}\right\| \leqslant 2\delta, \qquad s \in \{1,2,\ldots,d\}.$$

4. Для оставшихся $c \leqslant d$ биграмм выбираем такое значение $p(a_ia_j)T$, $i,j \in \{1,2,\ldots,m\}$, для которого разность $|\, p(a_ia_j)T - c\,|$ минимальна.

5. По найденному значению $p(a_ia_j)T$ однозначно определяем биграмму a_ia_j открытого текста, соответствующую биграмме $b_i^{(k)}b_j^{(l)}$ шифртекста.

6. Восстановив буквы открытого текста a_i, a_j из соотношения (1), определяем значения $\varepsilon_i, \varepsilon_j$.

7. Для определения центров $b_i^{(0)}$ и $b_j^{(0)}$ областей Π_i, Π_j решаем системы неравенств: $\|b_i^{(u_s)} + x\| \leqslant 2\varepsilon_i$, $s \in \{1,2,\ldots,m\}$ и $\|b_j^{(v_s)} + y\| \leqslant 2\varepsilon_j$, $s \in \{1,2,\ldots,c\}$.

Для полученных решений полагаем $b_i^{(0)} = x$ и $b_j^{(0)} = y$.

8. Восстанавливаем искомые области:

$$\Pi_i = \left\{z \in V_n : \|b_i^{(0)} + z\| \leqslant \varepsilon_i\right\}, \ \Pi_j = \left\{z \in V_n : \|b_j^{(0)} + z\| \leqslant \varepsilon_j\right\}.$$

З а м е ч а н и е. Точность предложенного метода определяется числом ложных биграмм (несоответствующих биграмме (a_ia_j), имеющих такое же расстояние $\chi \in \left[\chi_{ij}^{(k,l)} - 2\delta, \chi_{ij}^{(k,l)} + 2\delta\right]$, которые могут быть ошибочно учтены на шаге 2 алгоритма. Поэтому для повышения точности рассмотрим трехграмму $b_i^{(k)}b_j^{(l)}b_q^{(h)}$, где элемент $b_q^{(h)}$ следует за биграммой $b_i^{(k)}b_j^{(l)}$ в шифртексте. Аналогичным образом расширим

каждую из отобранных на шаге 2 биграмм и проведем дополнительную отбраковку с использованием уже трех расстояний из следующих интервалов:

$$\left[\chi_{ij}^{(k,l)} - 2\delta, \chi_{ij}^{(k,l)} + 2\delta\right], \quad \left[\chi_{iq}^{(k,h)} - 2\delta, \chi_{iq}^{(k,h)} + 2\delta\right], \quad \left[\chi_{qj}^{(h,l)} - 2\delta, \chi_{qj}^{(h,l)} + 2\delta\right].$$

Восстановив элементы a_i, a_j открытого текста и соответствующие области Π_i, Π_j пространства шифрвеличин, переходим к дешифрованию очередных биграмм шифртекста.

СПИСОК ЛИТЕРАТУРЫ

1. *Гридин В. Н.*, *Солодовников В. И.*, *Евдокимов И. А.* Применение нейросетевого подхода на основе LQV-сети для шифрования текстовой информации. Системы высокой доступности. М.: Радиотехника, 2011, № 7, с. 65–68.
2. *Гридин В. Н.*, *Солодовников В. И.*, *Евдокимов И. А.* Нейросетевой алгоритм симметричного шифрования. Информационные технологии. М.: Новые технологии, 2015, т. 21, № 4, с. 305–311.
3. *Духин А. А.* Теория информации. М.: Гелиос АРВ, 2007.
4. *Евдокимов И. А.*, *Солодовников В. И.* Анализ криптостойкости нейросетевого алгоритма симметричного шифрования. — Новые информационные технологии в автоматизированных системах, 2016, № 19, 263–269.
5. *Ивченко Г. И.*, *Медведев Ю. И.* Математическая статистика: Учеб. пособие для втузов. М.: Высшая школа, 1984, 248 с.