4 Элементы теории Шеннона

4.1 Модель противника

В 1949 г. была рассекречена и опубликована работа американского инженера-математика Клода Эдвуда Шеннона «Теория связи в секретных системах». В работе К. Шеннон совершил ряд открытий и предугаданий, которые позволили придать криптографии «математическое дыхание». В данной лекции мы остановимся только на нескольких результатах Шеннона из знаменитой работы.[1]

Шеннон рассматривал следующий сценарий атаки:

П1. Виктору известна криптосистема $C = \langle \mathcal{K}, \mathcal{X}, \mathcal{Y}, E, D \rangle$ (алгебраическая модель).

П2. Противник перехватывает все шифртексты.

П3. Ключ K и открытый текст X являются независимыми случайными величинами со следующими распределениями вероятностей:

$$p_K(\kappa) = \mathsf{P}\{K = \kappa\}, \quad \kappa \in \mathcal{K}, \quad p_X(x) = \mathsf{P}\{X = x\}, \quad x \in \mathcal{X}$$

(вероятностная модель).

С целью упрощения записи будем опускать индексы в p_K и p_X, предполагая, что на индекс однозначно указывает аргумент (κ или x). Будем считать, что $p(\kappa) > 0$ и $p(x) > 0$ для всех κ и x (все ключи и открытые тексты реализуемы).

П4. Противник обладает неограниченными вычислительными ресурсами.

Возникают вопросы:

1. Какие криптосистемы противостоят атакам по описанному сценарию?
2. Если криптосистема все-таки не является стойкой к атакам, то какое количество шифртекстов необходимо для проведения атаки?

Отметим, что предположение П1 поддерживает принцип Керкгоффса, а предположения П2, П3 — атаку при известном шифртексте (противнику известны статистические свойства открытого текста). Предположение П4 в современной криптографии звучит в другой форме: вычислительные ресурсы ограничены, однако, криптоаналитик обладает дополнительными данными и возможностями — знает некоторые открытые тексты, имеет возможность выбрать несколько открытых текстов и др.

4.2 Совершенные криптосистемы

Для случайных K и X шифртекст $Y = E_K(X)$ также оказывается случайной величиной с распределением вероятностей

$$p(y) = \sum_{x \in \mathcal{X}} p(y \mid x) p(x)$$

(использована формула полной вероятности), где

$$p(y \mid x) = \mathsf{P}\{Y = y \mid X = x\} = \sum_{\kappa \in \mathcal{K}:\ E_\kappa(x) = y} p(\kappa). \qquad (\star)$$

Лемма 4.1. Для любого $y \in \mathcal{Y}$: $p(y) > 0$.

[1] А.Н. Колмогоров: «Значение работ Шеннона для чистой математики не сразу было достаточно оценено. Мне вспоминается, что еще на международном съезде математиков в Амстердаме (1954 г.) мои американские коллеги, специалисты по теории вероятностей, считали мой интерес к работам Шеннона несколько преувеличенным, так как это более техника, чем математика. Сейчас такие мнения вряд ли нуждаются в опровержении. Правда, строгое математическое «обоснование» своих идей Шеннон в сколько-нибудь трудных случаях предоставил своим продолжателям. Однако, его математическая интуиция изумительно точна».

Доказательство. Следует из следующих фактов:

1. $p(x) > 0$ для любого $x \in \mathcal{X}$ (вероятностная модель);
2. $p(k) > 0$ для любого $k \in \mathcal{K}$ (вероятностная модель);
3. для любого $y \in \mathcal{Y}$ найдутся $x \in \mathcal{X}$ и $k \in \mathcal{K}$ такие, что $E_k(x) = y$ (определение криптосистемы, ограничение 2).

По формуле Байеса определим условное распределение

$$p(x \mid y) = \frac{p(x)p(y \mid x)}{p(y)}.$$

Определение 4.1 (совершенная криптосистема). Криптосистема C с введенными вероятностными распределениями $p(\kappa)$, $p(x)$ называется совершенной, если

$$p(x \mid y) = p(x), \quad \forall x \in \mathcal{X}, y \in \mathcal{Y}.$$

Неформально говоря, знание шифртекста не увеличивает информацию об открытом тексте.

Отметим, что по формуле полной вероятности

$$p(x, y) = p(x \mid y)p(y) = p(y \mid x)p(x)$$

и условие на совершенную криптосистему может быть заменено на следующее

$$p(y \mid x) = p(y), \quad \forall x \in \mathcal{X}, y \in \mathcal{Y}.$$

Его неформальная интерпретация также парадоксальна: шифртекст не содержит информации об открытом тексте.

Теорема 4.1. Если криптосистема C совершенна то

$$|\mathcal{X}| \leqslant |\mathcal{Y}| \leqslant |\mathcal{K}|.$$

Доказательство. Первое неравенство следует из того, что всякое преобразование зашифрования $E_\kappa \colon \mathcal{X} \to \mathcal{Y}$ является инъективным (в противном случае для некоторого X нарушается условие $D_\kappa(E_\kappa(X)) = X$).

Поскольку $p(y \mid x) = p(y) > 0$, из $(\star)$ следует, что для любого фиксированного x и любых y имеется не менее одного ключа κ такого, что $E_\kappa(x) = y$. Это значит, что

$$|\mathcal{Y}| = |\{E_\kappa(x) \colon \kappa \in \mathcal{K}\}| \leqslant |\mathcal{K}|.$$

Теорема 4.2. Если $|\mathcal{X}| = |\mathcal{Y}| = |\mathcal{K}|$, то криптосистема C совершенна тогда и только тогда, когда

1) уравнение $E_\kappa(x) = y$ однозначно разрешимо относительно $\kappa \in \mathcal{K}$ при любых $x \in \mathcal{X}$, $y \in \mathcal{Y}$;
2) $p(\kappa) = 1/|\mathcal{K}|$ для всех $\kappa \in \mathcal{K}$.

Доказательство. Необходимость. Из доказательства предыдущей теоремы следует, что

$$|\mathcal{Y}| = |\{E_\kappa(x) \colon \kappa \in \mathcal{K}\}| = |\mathcal{K}|.$$

Но это означает, что $E_\kappa(x) \neq E_{\kappa'}(x)$ для любых различных $\kappa, \kappa' \in \mathcal{K}$ и условие 1 доказано.

Для любых различных κ, κ' мы можем подобрать x и x' такие, что $E_\kappa(x) = E_{\kappa'}(x') = y$. Тогда из условия 1 и формулы $(\star)$ следует, что $p(y \mid x) = p(y) = p(y \mid x')$ только если $p(\kappa) = p(\kappa')$. Этим доказано условие 2.

Достаточность. Самостоятельно. □

Пример 4.1 (шифр Вернама, одноразовая лента). Пусть $\Sigma = \mathbb{Z}_m$. В шифре Вернама $C = \langle \Sigma^*, \Sigma^*, \Sigma^*, E, D \rangle$ длина ключа, открытого текста и шифртекста синхронизированы: если $E_K(X) = Y$, то $|K| = |X| = |Y|$. Зашифрование выполняется по правилу:

$$E_{\kappa_1\kappa_2\ldots\kappa_T}(x_1x_2\ldots x_T) = y_1y_2\ldots y_T, \quad y_t = x_t + \kappa_t.$$

Фактически мы имеем дело с шифром Виженера, в котором гамма не строится по ключу, а сама является ключом. Можно считать, что шифр Вернама — это шифр сдвига, в котором для зашифрования каждого нового символа открытого текста используется отдельный ключ κ_i. Шифр Вернама часто называется шифром одноразовой ленты.

Если в шифре Вернама символы κ_i выбираются случайно независимо равновероятно, то выполняются условия теоремы, т. е. это совершенная криптосистема. Недостатком криптосистемы является то, что длина ключа совпадает с длиной открытого текста. □

4.3 Энтропия

Напомним, что (двоичной) *энтропией* случайной величины X называется величина

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log_2 p(x) \quad (0 \cdot \log_2 0 = 0).$$

Условная энтропия:

$$H(X \mid y) = -\sum_{y} p(x \mid y) \log_2 p(x \mid y), \quad H(X \mid Y) = \sum_{y} p(y) H(X \mid y).$$

Напомним некоторые свойства энтропии:

1. $0 \leqslant H(X) \leqslant \log_2 |\mathcal{X}|$ (верхняя граница — для равномерного распределения, нижняя граница — для одноточечного).
2. $H(X, Y) \leqslant H(X) + H(Y)$ (равенство достигается, если X и Y независимы).
3. $H(X, Y) = H(Y) + H(X \mid Y)$.
4. Пусть $X_1, X_2, \ldots$ — последовательность независимых одинаково распределенных случайных величин со значениями в $\mathcal{X}$. Тогда можно построить последовательность подмножеств $B_n \subseteq \mathcal{X}^n$ такую, что при $n \to \infty$:

   а) множество $\mathcal{X}^n \setminus B_n$ имеет исчезающе малую вероятность, т. е. $\mathsf{P}\{X_1 X_2 \ldots X_n \notin B_n\} \to 0$;

   б) реализации из множества B_n становятся относительно равновероятными:

   $$\left| \frac{\log_2 \mathsf{P}\{X_1 \ldots X_n = b'\}}{\log_2 \mathsf{P}\{X_1 \ldots X_n = b\}} \right| \to 1, \quad \forall b, b' \in B_n;$$

   в) существует предел

   $$h = \lim_{n \to \infty} \frac{\log_2 |B_n|}{n},$$

   который называется *удельной энтропией*. Название объясняется следующим образом: $H(X_1, \ldots, X_n) \to hn$.

Пример 4.2. Пусть $X_1, X_2, \ldots$ имеют равномерное распределение. Тогда $B_n = \mathcal{X}^n$ и $h = \log_2 |\mathcal{X}|$. Понятно, что h принимает максимально возможное значение. □

Свойство 4 выполняется не только для последовательностей независимых одинаково распределенных случайных величин, но также и для так называемых *энтропийно устойчивых* последовательностей.

Пусть $\mathcal{X}$ — естественный алфавит (белорусский, английский), а $L \subseteq \mathcal{X}^*$ — осмысленный язык. Принято считать, что последовательности символов наудачу выбираемых из L слов являются энтропийно устойчивыми. Для некоторых естественных языков оценена их удельная энтропия h_L и рассчитана избыточность $R_L = 1 - \frac{h_L}{\log_2 |\mathcal{X}|}$:

характеристика	ru	fr	by
h_L	1.37	1.40	?
R_L	0.73	0.71	?

Пример 4.3. Шеннон предложил эвристическую оценку энтропии слов английского языка. Метод Шеннона был развит в американском стандарте NIST SP 800-63 для оценки энтропии паролей:

1. Энтропия первого символа пароля полагается равной 4.
2. Энтропия каждого из следующих 7 символов полагается равной 2.
3. Энтропия 9-го, 10-го,..., 20-го символов полагается равной 1.5.
4. Энтропия 21-го и последующих символов полагается равной 1. □

Пример 4.4. В современной криптографии оценка энтропии источников случайности является важной задачей. Проблемой является построение адекватной физической модели. В `http://comptop.stanford.edu/u/preprints/heads.pdf` построена модель «подбрасывания монетки». Согласно этой модели, монетка упадет на ту же грань, с которой она была подброшена, с вероятностью ≈ 0.51. □

4.4 Расстояние единственности

Теорема 4.3. Для криптосистемы C с введенными вероятностными распределениями $p(\kappa)$, $p(x)$ выполняется:

$$H(K \mid Y) = H(X) + H(K) - H(Y).$$

Доказательство. Так как открытый текст и ключ выбираются независимо

$$H(X, K) = H(X) + H(K).$$

С другой стороны, знание X и K или Y и K эквивалентно знанию всех трех величин X, Y, K. Поэтому

$$H(X, K) = H(Y, K) = H(Y) + H(K \mid Y)$$

Собирая оба полученных равенства, получаем требуемый результат. □

Пусть выполняется зашифрование открытых текстов $X_1, X_2, \dots X_T$ на одном и том же ключе K.

Определение 4.2. *Расстоянием единственности* T_0 криптосистемы C называется минимальное T такое, что

$$H(K \mid Y_1, Y_2, \dots, Y_T) = 0$$

(расстояние может равняться ∞). □

Как и при доказательстве теоремы можно показать, что

$$H(K \mid Y_1 Y_2 \dots Y_T) = H(X_1 X_2 \dots X_T) + H(K) - H(Y_1 Y_2 \dots Y_T)$$

и расстояние единственности T_0 близко к решению уравнения

$$H(K) = H(Y_1 Y_2 \dots Y_T) - H(X_1 X_2 \dots X_T)$$

относительно T.

Выдвинем следующие предположения:

а) криптосистема C эндоморфна;

б) ключ K выбирается равновероятно и $H(K) = \log_2 |\mathcal{K}|$;

в) шифртексты имеют высокую энтропию и $H(Y_1 Y_2 \dots Y_T) \approx T \log_2 |\mathcal{X}|$;

г) слово $X_1 X_2 \dots X_T$ выбирается наудачу из L, T достаточно велико и $H(X_1 X_2 \dots X_T) \approx T h_L$.

При этом искомое расстояние единственности

$$t_0 \approx \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{X}| - h_L} = \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{X}|}.$$