ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 51 2015 Вып. 1

УДК 621.391.1

© 2015 г. **Б.Я. Рябко**

ШИФР ВЕРНАМА УСТОЙЧИВ К НЕБОЛЬШИМ ОТКЛОНЕНИЯМ ОТ СЛУЧАЙНОСТИ[1]

Шифр Вернама, или "одноразовый блокнот", играет важную роль в криптографии, так как он является совершенным, или совершенно секретным. В этом шифре ключ является последовательностью равновероятных и независимо порожденных символов. Показано, что при небольших нарушениях этих свойств получаемый шифр близок к шифру Вернама в случае, когда шифруемый текст и ключевая последовательность порождаются стационарными эргодическими источниками.

§ 1. Введение

Рассматривается классическая проблема передачи секретных сообщений от передатчика (Алисы) к получателю (Бобу) по открытой линии связи, сообщения в которой может читать злоумышленник (Ева). Алиса и Боб (но не Ева) знают так называемый ключ, который является словом в некотором алфавите. Перед передачей сообщения Бобу Алиса шифрует его, а Боб после получения зашифрованного сообщения его дешифрует.

Будем рассматривать так называемые шифры с бегущим ключом (running-key ciphers), в которых исходный текст $X_1 \dots X_t$, ключевая последовательность $Y_1 \dots Y_t$ и зашифрованная последовательность $Z_1 \dots Z_t$ принадлежат одному алфавиту $A = \{0, 1, \dots, n-1\}$, где $n \geqslant 2$. Предполагается, что шифрование и дешифрование определяются равенствами

$$Z_i = c(X_i, Y_i), \quad i = 1, \dots, t,$$
$$X_i = d(Z_i, Y_i), \quad i = 1, \dots, t,$$

так что $d(e(X_i, Y_i), Y_i) = X_i$. Функции c и d называются кодером и декодером. Часто кодер и декодер задаются равенствами

$$Z_i = (X_i + Y_i) \mod n, \quad X_i = (Z_i - Y_i) \mod n, \tag{1}$$

т.е. $c(X_i, Y_i) = (X_i + Y_i) \bmod n$, $d(Z_i, Y_i) = (Z_i - Y_i) \bmod n$. В случае $n = 2$ соотношение (1) может быть представлено в виде

$$Z_i = (X_i \oplus Y_i), \quad X_i = (Z_i \oplus Y_i), \tag{2}$$

где $a \oplus b = (a + b) \bmod 2$.

Шифр с бегущим ключом (1) называется шифром Вернама (или одноразовым блокнотом), если символы ключевой последовательности равновероятны и независимы, т.е. для каждого слова $k_1 \dots k_t$, $k_i \in A$, выполнено $P(Y_1 \dots Y_t = k_1 \dots k_t) = n^{-t}$.

[1] Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 12-07-00125).

Этот шифр играет важную роль в криптографии, так как он совершенно секретен [1]. Это означает, что

$$P(X_1 \dots X_t) = P(X_1 \dots X_t \,|\, Z_1 \dots Z_t)$$

для всех $X_1 \dots X_t \in A^t$, $Z_1 \dots Z_t \in A^t$, т.е. неформально неопределенность о передаваемом тексте $X_1 \dots X_t$ не меняется при известном зашифрованном сообщении $Z_1 \dots Z_t$. Используя энтропию Шеннона, это свойство можно представить в виде

$$h(X_1 \dots X_t) = h(X_1 \dots X_t \,|\, Z_1 \dots Z_t),$$

где $h(X_1 \dots X_t)$ и $h(X_1 \dots X_t \,|\, Z_1 \dots Z_t)$ – безусловная и условная энтропии исходного сообщения $X_1 \dots X_t$.

Если текст порождается стационарным эргодическим источником, то совершенная секретность шифра Вернама имеет простую интерпретацию, поясняющую смысл этого понятия. Как следует из известной теоремы Шеннона – Макмиллана – Бреймана, все множество сообщений $X_1 \dots X_t$ при больших t можно разбить на две части: $2^{h(X_1 \dots X_t)}$ сообщений, вероятности которых близки по величине и в сумме дают почти единицу, и множество остальных сообщений, суммарная вероятность которых близка к нулю. Ева знает, что почти наверное зашифрованное сообщение принадлежит первому подмножеству, но все сообщения в этом подмножестве имеют близкие вероятности, причем количество таких сообщений растет экспоненциально (как 2^{ht}, где h – энтропия источника сообщений). Именно по этой причине Ева не может определить исходное сообщение.

В данной статье рассматривается случай, когда ключевая последовательность порождается стационарным эргодическим источником и немного отличается от равновероятных и независимых символов. Показано, что свойства такого шифра остаются в определенном смысле близкими к шифру Вернама. Точнее, показано, что в этом случае множество близких по вероятности сообщений, суммарная вероятность которых близка к единице, растет как $2^{t(h-r)}$, где по-прежнему h – энтропия источника, а r – избыточность источника ключа, равная $\log n - h_{\text{key}}$, где n – число букв алфавита, h_{key} – энтропия источника ключа. Если избыточность приближается к нулю, то число элементов в высоковероятном множестве приближается к 2^{ht}, т.е. к шифру Вернама. Это и позволяет утверждать, что шифр Вернама устойчив к малым отклонениям. Отметим, что сейчас мы неформально оценили степень отклонения избыточностью ключевой последовательности: чем она меньше, тем меньше отклонения. Однако далее мы дадим и более формальное обоснование: в данном случае избыточность совпадает с расстоянием по Кульбаку – Лейблеру, широко используемым в теории информации для количественной оценки различий между распределениями вероятностей.

Интересно, что Шеннон в своей основополагающей работе [1] отметил, что "с криптографической точки зрения секретная система почти тождественна системе связи при наличии шума". Поэтому с математической точки зрения задачи дешифрования текстов и фильтрации случайных процессов очень близки. Развиваемый в настоящей статье подход близок к методам, использованным в работе [2], в которой рассматривается задача фильтрации стационарных процессов.

§ 2. Предварительные сведения

Рассматривается случай, когда шифруемый текст $X = X_1 X_2 \dots$ и последовательность ключа $Y_1 Y_2 \dots$ независимо генерируются стационарными эргодическими процессами с одинаковым конечным алфавитом $A = \{0, 1, \dots, n-1\}$, $n \geqslant 2$, а $Z = Z_1 Z_2 \dots$ определяется соотношением (1).

Энтропия Шеннона m-го порядка и предельная энтропия задаются равенствами

$$h_m(X) = -\frac{1}{m+1} \sum_{u \in A^{m+1}} P_X(u) \log P_X(u), \quad h(X) = \lim_{m \to \infty} h_m(X), \tag{3}$$

где $m \geqslant 0$, $P_X(u)$ – вероятность того, что $X_1 X_2 \dots X_{|u|} = u$ (здесь предел всегда существует [3,4]). Определим также условную энтропию

$$h_m(X \,|\, Z) = h_m(X, Z) - h_m(Z), \quad h(X \,|\, Z) = \lim_{m \to \infty} h_m(X \,|\, Z). \tag{4}$$

Для двух распределений вероятностей P и Q, определенных на некотором алфавите $A = \{a_1, \dots, a_n\}$, $n \geqslant 2$, расхождение по Кульбаку – Лейблеру (см. [3]) определяется равенством

$$D(P \,\|\, Q) = \sum_{a \in A} P(a) \log(P(a)/Q(a)).$$

Для двух стационарных процессов $U = U_1 U_2 \dots$ и $V = V_1 V_2 \dots$ расхождение по Кульбаку – Лейблеру m-го порядка и предельное расхождение определяются равенствами

$$D(U \,\|\, V)_m = -\frac{1}{m} \sum_{w \in A^m} P(U_1 \dots U_m = w) \log(P(U_1 \dots U_m = w)/P(V_1 \dots V_m = w)),$$

$$D(U, V) = \lim_{m \to \infty} D(U \,\|\, V)_m.$$

Из этих равенств и (3) легко видеть, что если V порождает независимые и равновероятные символы из n-буквенного алфавита A, то

$$D(U \,\|\, V) = \log n - h(U).$$

Эту величину, широко известную в теории информации и называемую избыточностью процесса U, будем в дальнейшем обозначать через r_U:

$$r_U = \log n - h(U). \tag{5}$$

Далее "близость" процессов будет оцениваться расхождением по Кульбаку – Лейблеру, которое в интересующем нас случае совпадает с избыточностью.

В теории информации широко известна [3,4] следующая

Т е о р е м а 1 (Шеннона – Макмиллана – Бреймана). *Пусть $U = U_1 U_2 U_3 \dots$ – стационарный эргодический процесс. Тогда $\forall\, \varepsilon > 0$, $\forall\, \delta > 0$, для почти всех $U_1 U_2 U_3 \dots$ существует n', такое что при $n > n'$*

$$P\left\{\left| -\frac{1}{n} \log P(U_1 \dots U_n) - h(U) \right| < \varepsilon \right\} \geqslant 1 - \delta, \tag{6}$$

где $P(U_1 \dots U_n)$ – вероятность $U_1 \dots U_n$.

§ 3. Основной результат

Т е о р е м а 2. *Пусть текст $X = X_1 X_2 \dots$ и ключ $Y = Y_1 Y_2 \dots$ – независимые процессы с алфавитом $A = \{0, 1, \dots, n-1\}$, $n \geqslant 2$, такие что процесс $(X, Y) = (X_1, Y_1), (X_2, Y_2), \dots$ – стационарный и эргодический, а $Z = Z_1, Z_2, \dots$ определяется соотношением (1). Тогда с вероятностью 1 для каждого $\varepsilon > 0$ и $\delta > 0$ существует такое целое n', что для каждого $t > n'$ и $Z_1^t = Z_1, Z_2, \dots Z_t$ существует множество $\Psi(Z_1^t)$ текстов длины t, для которого*

i) $P(\Psi(Z_1^t)) > 1-\delta$;
ii) *Для каждых* $X^1 = X_1^1 \dots X_t^1$, $X^2 = X_1^2 \dots X_t^2$ *из* $\Psi(Z_1^t)$

$$\frac{1}{t}\left|\log P(X^1 \mid Z_1^t) - \log P(X^2 \mid Z_1^t)\right| < \varepsilon;$$

iii) $\liminf\limits_{t\to\infty} \frac{1}{t}\log|\Psi(Z_1^t)| \geqslant h(X \mid Z)$.

Доказательство. Так как процесс (X, Z) является детерминированной функцией процесса (X, Y), то из эргодичности и стационарности процесса (X, Y) следует эргодичность и стационарность процесса (X, Z).

Перейдем к построению множества $\Psi(Z_1^t)$. Для этого применим теорему Шеннона – Макмиллана – Бреймана, но сначала заметим, что

$$h(X \mid Z) = h(X, Z) - h(Z)$$

и

$$\log P(X_1 \dots X_n \mid Z_1 \dots Z_n) = \log P(X_1 \dots X_n; Z_1 \dots Z_n) - \log P(Z_1 \dots Z_n).$$

Применяя неравенство (6) к $\log P(X_1 \dots X_n; Z_1 \dots Z_n)$, $h(X, Z)$ и $\log P(Z_1 \dots Z_n)$, $h(Z)$, теорему Шеннона – Макмиллана – Бреймана можно записать следующим образом: $\forall\,\varepsilon > 0, \forall\,\delta > 0$, для почти всех $(X_1, Z_1), (X_2, Z_2), \dots$ существует n', такое что при $n > n'$

$$P\left\{\left|-\frac{1}{n}\log P(X_1 \dots X_n \mid Z_1 \dots Z_n) - h(X \mid Z)\right| < \varepsilon\right\} \geqslant 1-\delta. \tag{7}$$

Отсюда для любых $\varepsilon > 0$, $\delta > 0$ и почти всех Z существует такое n', что для $t > n'$

$$P\left\{\left|-\frac{1}{t}\log P(X_1 X_2 \dots X_t \mid Z_1 Z_2 \dots Z_t) - h(X \mid Z)\right| < \varepsilon/2\right\} \geqslant 1-\delta. \tag{8}$$

Определим

$$\Psi(Z_1^t) = \{X = X_1 X_2 \dots X_t : |P(X_1 X_2 \dots X_t \mid Z_1 Z_2 \dots Z_t) - h(X \mid Z)| < \varepsilon/2\}. \tag{9}$$

Свойство i) теоремы немедленно следует из (8). Для доказательства свойства ii) заметим, что для $X^1 = X_1^1 \dots X_t^1$, $X^2 = X_1^2 \dots X_t^2$ из $\Psi(Z_1^t)$ из (8), (9) получаем

$$\frac{1}{t}\left|\log P(X^1 \mid Z_1^t) - \log P(X^2 \mid Z_1^t)\right| \leqslant \frac{1}{t}\left|\log P(X^1 \mid Z_1^t) - h(X \mid Z)\right| +$$
$$+ \frac{1}{t}\left|\log P(X^2 \mid Z_1^t) - h(X \mid Z)\right| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

Из (9) и свойства i) получаем

$$|\Psi(Z_1^t)| > (1-\delta)2^{t(h(X\mid Z)-\varepsilon)}.$$

Учитывая, что это выполняется для любых $\varepsilon > 0$, $\delta > 0$ и $t > n'$, получаем свойство iii). ▲

Таким образом, множество возможных расшифровок $\Psi(Z_1^t)$ растет экспоненциально, его суммарная вероятность близка к единице, и вероятности слов внутри этого множества близки по величине.

Приведенная теорема дает возможность оценить характеристики шифра с помощью условной энтропии $h(X \mid Z)$. Следующие оценки не требуют вычисления условной энтропии, а основаны на величинах, вычисляемых проще.

Следствие. *Для почти всех $Z_1Z_2\ldots$ справедливы неравенства*

$$\liminf_{t\to\infty}\frac{1}{t}\log|\Psi(Z_1^t)|\geqslant h(X)+h(Y)-\log n, \tag{10}$$

$$h(X\,|\,Z)\geqslant h(Y)+h(X)-\log n. \tag{11}$$

Доказательство. Из хорошо известного представления $h(X,Z)=h(X)+h(Z\,|\,X)$ (см. [3,4]) получаем

$$h(X\,|\,Z)=h(X,Z)-h(Z)=h(Z\,|\,X)+h(X)-h(Z).$$

Учитывая, что $\max h(Z)=\log n$ (см. [3,4]), где n – число букв алфавита, из последнего равенства получаем

$$h(X\,|\,Z)\geqslant h(Z\,|\,X)+h(X)-\log n.$$

Из независимости X и Y и определения шифра с бегущим ключом (1) видно, что $h(Z\,|\,X)=h(Y)$. Отсюда и предыдущего неравенства получаем (11). Из свойства iii) теоремы 2 и неравенства (11) следует (10). ▲

Замечание. Используя ранее введенное понятие избыточности, можно выразить скорость роста множества $\frac{1}{t}\log|\Psi(Z_1^t)|$ следующим образом:

$$\begin{aligned}
&\liminf_{t\to\infty}\frac{1}{t}\log|\Psi(Z_1^t)|\geqslant h(X)-r_Y,\\
&\liminf_{t\to\infty}\frac{1}{t}\log|\Psi(Z_1^t)|\geqslant h(Y)-r_X,\\
&\liminf_{t\to\infty}\frac{1}{t}\log|\Psi(Z_1^t)|\geqslant \log n-(r_X+r_Y),
\end{aligned} \tag{12}$$

где $r_Y=\log n-h(Y)$ и $r_X=\log n-h(X)$ – избыточности. Кроме того, из определения избыточности (5) и неравенства (11) получаем

$$h(X\,|\,Z)\geqslant h(Y)-r_X.$$

Эти неравенства позволяют количественно оценить влияние избыточности на стойкость шифра и подтверждают известный в криптографии и теории вероятности факт: уменьшение избыточности повышает надежность шифра.

Вернемся теперь к вопросу о влиянии отклонений от случайности ключевой последовательности шифра Вернама. Пусть шифруемый текст – $X_1X_2\ldots$, $X_i\in\{0,1\}$, и пусть последовательность символов ключа $Y_1Y_2\ldots$, $Y_i\in\{0,1\}$, генерируется источником, отличным от источника Бернулли с $P(0)=P(1)=0{,}5$. (Например, ключ $Y_1Y_2\ldots$ генерируется бернуллиевским источником с вероятностями символов $P(0)=0{,}5-\tau$, $P(1)=0{,}5+\tau$, где τ – небольшое число.) Из (12) можно видеть, что величина множества высоковероятных расшифровок $\Psi(Z_1^t)$ растет экспоненциально с показателем, не меньшим $h(X)-r_Y$, где $r_Y=1-h(Y)$ – избыточность. Видно, что если r_Y стремится к нулю, то размер множества высоковероятных расшифровок приближается к величине соответствующего множества в шифре Вернама. Действительно, $h(Y)=1$, и следовательно, избыточность $r_Y=0$, как в шифре Вернама. Неформально можно сказать, что шифр Вернама устойчив к небольшим отклонениям от случайности ключа.

СПИСОК ЛИТЕРАТУРЫ

1. *Шеннон К.* Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. М.: Изд-во иностр. лит., 1963.

2. *Ryabko B., Ryabko D.* Confidence Sets in Time-Series Filtering // Proc. 2011 IEEE Int. Sympos. on Information Theory (ISIT'2011). St. Petersburg, Russia. July 31 – August 5, 2011. P. 2509–2511.
3. *Cover T.M., Thomas J.A.* Elements of Information Theory. New York: Wiley-Interscience, 2006.
4. *Галлагер Р.* Теория информации и надежная связь. М.: Сов. радио, 1974.

Рябко Борис Яковлевич
Сибирский государственный университет
телекоммуникаций и информатики
Институт вычислительных технологий Сибирского отделения РАН
rbya@yandex.ru

Поступила в редакцию
07.04.2014
После переработки
25.11.2014