УДК 621.391

А.Б. Лось

Исследование информационных характеристик преобразований замены и перестановки

Излагаются результаты исследования информационных характеристик преобразований замены и перестановки, являющихся основой построения криптографических алгоритмов. Получены оценки взаимной информации входных и выходных сообщений дискретного канала связи при применении указанных преобразований.

Ключевые слова: канал связи, взаимная информация, преобразование замены и перестановки.

В настоящей статье излагаются результаты исследования информационных характеристик преобразований замены и перестановки, являющихся основой построения криптографических алгоритмов [1−2]. Для указанных преобразований найдены верхние оценки взаимной информации входных и выходных сообщений дискретного канала связи. Полученные результаты позволяют оценивать эффективность данных преобразований в различных криптографических ситуациях.

Пусть знаки a_i входного сообщения $S_n \in \sigma(n)$ длины N: $\overline{a}_N = (a_1,...,a_N)$ дискретного канала связи, выбираются из алфавита $A = \{1,2,...,n\}$, $a_i \in A$, $i = 1,2,...,N$, а знаки b_i выходного сообщения $\overline{b}_N$, $\overline{b}_N = (b_1,...,b_N)$ образуются из знаков сообщения $\overline{a}_N$ путем применения преобразований замены и перестановки, выражаемых уравнениями:

$$b_i = a_i S, \tag{1}$$

$$b_i = a_{s(i)}, \quad i = 1,2,...,N, \tag{2}$$

где S_n − некоторая подстановка степени n, выбираемая из множества $\sigma(n)$ − всех подстановок степени n; а $S_N = \begin{pmatrix} 1, ..., N \\ s(1),...,s(N) \end{pmatrix}$ − некоторая подстановка степени N, выбираемая из множества $\sigma(N)$ всех подстановок степени N.

Обозначим через $M^N = \{\overline{a}_N\}$ и $E^N = \{\overline{b}_N\}$ множества входных и выходных сообщений длины N соответственно.

Зададим на множестве входных сообщений M^N и множествах подстановок $\sigma(n)$ и $\sigma(N)$ некоторые вероятностные распределения:

$$p(M^N) = \{p(\overline{a}_N), \overline{a}_N \in M^N\},$$
$$p(\sigma(n)) = \{p(S_n), S_n \in \sigma(n)\},$$
$$p(\sigma(N)) = \{p(S_N), S_N \in \sigma(N)\}.$$

Нетрудно видеть, что при этом в том и другом случае будут индуцироваться некоторые вероятностные распределения на множестве выходных сообщений E^N.

Назовем далее $H(A)$ − энтропию вероятностной схемы (ансамбля) A; $H(A/B)$ − условную энтропию ансамбля A при заданном ансамбле B, а $I(A,B)$ − взаимную информацию ансамблей A и B.

Пользуясь известными свойствами энтропии [3−4], получаем

$$H(M^N) + H(E^N/M^N) = H(E^N) + H(M^N/E^N),$$

откуда следует равенства:

$$H(M^N/E^N) = H(M^N) - H(E^N) + H(E^N/M^N), \tag{3}$$

$$I(A,B) = H(M^N) - H(M^N/E^N) = H(E^N) - H(E^N/M^N), \tag{4}$$

где

$$H(M^N) = -\sum_{\overline{a}_N \in M^N} p(\overline{a}_N) \cdot \log p(\overline{a}_N), \tag{5}$$

$$H(E^N)=-\sum_{\bar{b}_N\in M^N} p(\bar{b}_N)\cdot\log p(\bar{b}_N)\,, \tag{6}$$

а логарифм берется по основанию 2.

Рассмотрим вначале задачу оценки взаимной информации для преобразования замены.

В соответствии с определением условной энтропии получаем:

$$H(E^N/M^N)=-\sum_{\bar{a}_N\in M^N}\sum_{\bar{b}\in M^N} p(\bar{a}_N)\cdot p(\bar{b}_N/\bar{a}_N)\cdot\log p(\bar{b}_N/\bar{a}_N)\,, \tag{7}$$

где

$$p(\bar{b}_N)=\sum_{\bar{a}_N\in M^N} p(\bar{a}_N)\cdot p(\bar{b}_N/\bar{a}_N)\,, \tag{8}$$

$$p(\bar{b}_N/\bar{a}_N)=\sum_{S_n\in\sigma(n)} p(S_N)\cdot I\{b_i=a_iS_N,\ i=\overline{1,N}\}\,,$$

$I(R)$ – индикатор условия R.

Дальнейшие расчеты будем проводить в предположении, что рассматриваемый канал связи есть дискретный канал без памяти, при этом, очевидно,

$$p(\bar{a}_N)=p(a_1)\cdot\ldots\cdot p(a_N)\,,$$

а также в предположении, что подстановка S_n выбирается случайно и равновероятно из множества $\sigma(n)$ – всех подстановок степени n.

В этом случае:

$$p(\bar{b}_N/\bar{a}_N,S_n)=\sum_{S_n\in\sigma(n)} p(S_n)p(\bar{b}_N/\bar{a}_N,S_n)=\frac{1}{n!}\sum_{S_n\in\sigma(n)} p(\bar{b}_N/\bar{a}_N,S_n),$$

где $p(\bar{b}_N/\bar{a}_N,S_n)=1$, если $b_i=a_iS_n$, $i=1,2,\ldots,N$ и 0 – в противном случае.

Последнее соотношение можно переписать в виде условий:

$$p(\bar{b}_N/\bar{a}_N,S_n)=\frac{[n-\upsilon(b_1,\ldots,b_N)]!}{n!}, \tag{9}$$

если существует такая подстановка $S_n\in\sigma(n)$, что $b_i=a_iS_n$, $i=1,\ldots,N$; $p(\bar{b}_N/\bar{a}_N,S_n)=0$ в противном случае, где $\upsilon=\upsilon(b_1,\ldots,b_N)$ – число различных элементов в последовательности $(b_1,\ldots,b_N)$.

Пусть далее $(\alpha(1),\ldots,\alpha(n))$ – первичная спецификация последовательности $(b_1,\ldots,b_N)$, а именно: $\alpha(r)$ – число элементов последовательности $(b_1,\ldots,b_N)$, равных r, $r=1,\ldots,n$.

Тогда из (9) получаем:

$$p(\overline{\bar{b}_N})=\frac{[n-\upsilon(b_1,\ldots,b_N)]!}{n!}\sum_{\substack{r_1,\ldots,r_\upsilon=1\\ r_i\neq r_j,\,i\neq j}}^{n}\prod_{\ell=1}^{\upsilon}[p(r_l)]^{\alpha(r_l)}, \tag{10}$$

где $\alpha(r_k)>0$, $k=1,2,\ldots,\upsilon$, т.е. $\alpha(r_k)$ – элементы последовательности первичной спецификации, отличные от 0.

Подставляя (10) в (6) и (7), получаем

$$H(E^N/M^N)=-\sum_{\substack{l_1,\ldots,l_n=0\\ l_1+\ldots+l_n=N}}^{N}\frac{N!}{l_1!\ldots l_n!}p(1)^{l_1}\ldots p(n)^{l_n}\times\sum_{\substack{k(1),\ldots,k(\mu(l_1,\ldots,l_n))=1\\ k(i)\neq k(j),\,i\neq j}}^{n}\frac{[n-\mu(l_1,\ldots,l_n)]!}{n!}\cdot\log\frac{[n-\mu(l_1,\ldots,l_n)]!}{n!}. \tag{11}$$

$$H(E^N)=-\sum_{\substack{l_1,\ldots,l_n=0\\ l_1+\ldots+l_n=N}}^{N}\frac{N!}{l_1!\ldots l_n!}\frac{(n-\mu(l_1,\ldots,l_n))!}{n!}\sum_{\substack{r(1),\ldots,r(\mu)=1\\ r(i)\neq r(j)}}^{n}\prod_{k=1}^{\mu(l_1,\ldots,l_n)}[p(r(k))]^{l(r(k))}\times$$

$$\times\log_2\frac{(n-\mu(l_1,\ldots,l_n))!}{n!}\sum_{\substack{r(1),\ldots,r(\mu)=1\\ r(i)\neq r(j)}}^{n}\prod_{k=1}^{\mu(l_1,\ldots,l_n)}[p(r(k))]^{l(r(k))}, \tag{12}$$

где $\mu=\mu(l_1,\ldots,l_n)$ – число ненулевых элементов в последовательности $(l_1,\ldots l_n)$, $(l(r(1),\ldots,l(r(\mu))$ – последовательность самих ненулевых элементов.

Подставляя (11) и (12) в равенство (4), получаем выражение для взаимной информации входных и выходных сообщений рассматриваемого канала связи $I(M^N,E^N)$, явный вид которого, в силу громоздкости выражений, приведем для случая $p(a_i)=1/n,\ i=1,...,n$:

$$I(M^N,E^N)=N\log n-n^{-N}\cdot\sum_{\substack{l_1,...,l_n=0\\ l_1+...+l_n=N}}^{N}\frac{N!}{l_1!...l_n!}\log\frac{n!}{(n-\mu(l_1,...,l_n))!}. \qquad (13)$$

В силу очевидных неравенств

$$H(M^N/E^N)>n^{-N}\cdot\begin{pmatrix}n\\N\end{pmatrix}N!\cdot\log\frac{n!}{(n-N)!},$$

$$-x>\ln(1-x)>\frac{x}{x-1},\quad 0<x<1,$$

из соотношения (12), в условиях $n>N$, получаем оценку для $I(M^N,E^N)$ – величины взаимной информации входных и выходных сообщений при применении преобразования простой замены:

$$\frac{1}{N}I(M^N,E^N)\le\frac{N^2}{n-N}\left[1+\log n\right]. \qquad (14)$$

Рассмотрим теперь преобразование перестановки.

Заметим, что в соответствии с введенными выше предположениями, вероятность появления входного сообщения $\bar{a}_n=(a_1,...,a_n)$, где $a_i\in A=\{1,...,n\}$, равна

$$p(\bar{a}_N)=p(a_1)\cdot...\cdot p(a_N)=p_1{}^{r_1}...\,p_n{}^{r_n}, \qquad (15)$$

где p_k – вероятность появления знака входного сообщения равного k, а вектор частот $\bar{r}=(r_1,...,r_n)$ – первичная спецификация последовательности $\bar{a}_N$, $r_к$ – число исходов, равных k. Будем также предполагать, что подстановка S_N выбирается случайно и равновероятно из множества $\sigma(N)$ – всех подстановок степени N.

Нетрудно видеть, что все множество входных сообщений M^N можно представить в виде объединения непересекающихся множеств $M^N(\bar{r})$, соответствующих первичным спецификациям векторов $\bar{r}$:

$$M^N=\underset{\bar{r}}{U}M^N(\bar{r}).$$

Аналогичным образом можно представить и множество выходных сообщений E^N:

$$E^N=\underset{\bar{r}}{U}E^N(\bar{r}).$$

Далее заметим, что условная вероятность $p(\bar{b}_N/\bar{a}_N)$ появления выходного сообщения $\bar{b}_N$ при заданном входном сообщении $\bar{a}_N\in M^N(\bar{r})$ имеет вид

$$p(\bar{b}_N/\bar{a}_N)=\frac{r_1!...r_n!}{N!},\ \text{если}\ \bar{b}_N\in E^N(\bar{r}),$$

$$p(\bar{b}_N/\bar{a}_N)=0,\ \text{если}\quad \bar{b}_N\notin E^N(\bar{r}). \qquad (16)$$

Следовательно, при $\bar{b}_N\in E^N(\bar{r})$

$$p(\bar{b}_N)=\sum_{\bar{a}_N\in M^N}p(\bar{a}_N)\,p(\bar{b}_N/\bar{a}_N)=\sum_{\bar{a}_N\in M^N(\bar{r})}p_1{}^{r_1}...p_n{}^{r_n}\frac{r_1!...r_n!}{N!}=p_1{}^{r_1}...p_n{}^{r_n}. \qquad (17)$$

Для энтропии $H(E^N)$ ансамбля выходных сообщений имеем

$$H(E^N)=-\sum_{\bar{b}_N\in E^N}p(\bar{b}_N)\log p(\bar{b}_N)=-\sum_{\substack{\bar{r}=(r_1,...,r_n)\\ r_1+...+r_n=N}}\ \sum_{\bar{b}_N\in E^N(\bar{r})}p_1{}^{r_1}...p_n{}^{r_n}\log(p_1{}^{r_1}...p_n{}^{r_n})=$$

$$=-\sum_{\substack{\bar{r}=(r_1...r_n)\\ r_1+...+r_n=N}}\frac{N!}{r_1!...r_n!}p_1{}^{r_1}...p_n{}^{r_n}\log[p_1{}^{r_1}...p_n{}^{r_n}]. \qquad (18)$$

В соответствии с определением условной энтропии имеет место равенство

$$H(E^N/M^N)=-\sum_{\bar{a}_N\in M^N}p(\bar{a}_N)\sum_{\bar{b}_N\in E^N}p(\bar{b}_N/\bar{a}_N)\log p(\bar{b}_N/\bar{a}_N)=$$

$$=-\sum_{\substack{\bar{r}=(r_1,\dots r_n)\\ r_1+\dots r_n=N}}\sum_{\substack{\bar{a}_N\in M^N(\bar{r})\\ \bar{b}_N\in E^N(\bar{r})}}p_1^{r_1}\dots p_n^{r_n}\frac{r_1!\dots r_n!}{N!}\log\left(\frac{r_1!\dots r_n!}{N!}\right)=\sum_{\substack{\bar{r}=(r_1,\dots,r_n)\\ r_1+\dots+r_n=N}}p_1^{r_1}\dots p_n^{r_n}\frac{N!}{r_1!\dots r_n!}\log\left(\frac{N!}{r_1!\dots r_n!}\right). \tag{19}$$

С учетом (4), (18) и (19) получаем

$$H(E^N/M^N)-H(E^N)=\sum_{\substack{\bar{r}=(r_1,\dots r_n)\\ r_1+\dots r_n=N}}\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\left[\log\left(\frac{N!}{r_1!\dots r_n!}\right)+\log(p_1^{r_1}\dots p_n^{r_n})\right]=$$

$$=\sum_{\substack{\bar{r}=(r_1,\dots r_n)\\ r_1+\dots r_n=N}}\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\log\left[\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\right]. \tag{20}$$

С учетом (20) из соотношения (4) получаем

$$I(M^N,E^N)=H_N(p_1,\dots p_n), \tag{21}$$

где

$$H_N(p_1,\dots,p_n)=-\sum_{\substack{\bar{r}=(r_1,\dots r_n)\\ r_1+\dots r_n=N}}\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\log\left[\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\right] \tag{22}$$

есть энтропия полиномиального распределения.

Далее в работе исследуется асимптотическое поведение величины $H_N(p_1,\dots,p_n)$ при $N\to\infty$ и $n/N\to 0$.

Рассмотрим полиноминальную схему с числом испытаний $N\to\infty$ и вектором вероятностей $P=(P_1,\dots,P_n)$, где P_k – вероятность появления исхода, равного k, $k=1,\dots,n$.

Обозначим через ξ_k случайную величину, равную числу исходов в данной полиноминальной схеме, равных k, $k=1,\dots,n$.

Тогда, очевидно,

$$P(\xi_k=k)=P_k,\ \ E\xi_k=NP_k,\ D\xi_k=NP_k(1-P_k),\ \ k=1,\dots,n,$$

$$P(\xi_1=r_1,\dots,\xi_n=r_n)=\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}. \tag{23}$$

Учитывая соотношение (23), величину $H_N(P_1,\dots,P_n)$ можно представить в виде

$$H_N(P_1,\dots,P_n)=-\log N!+\sum_{k=1}^{n}E\log(\xi_k!)-\sum_{k=1}^{n}E\xi_k\log P_k. \tag{24}$$

Нетрудно видеть, что

$$\sum_{k=1}^{n}E\xi_k\log P_k=N\cdot H_p, \tag{25}$$

где $H_p=\sum_{k=1}^{n}P_k\log P_k$.

Для оценки первого слагаемого в (24) используем формулу Стирлинга ([5]):

$$x!=\sqrt{2\pi}x^{x+1/2}e^{-x+\theta/12x}, \tag{26}$$

где $x>0$, $0<\theta<1$.

Тогда

$$\log N!=N\log N+\frac{1}{2}\log N-N\log e+\log\sqrt{2\pi}+\frac{\theta}{12N}\log e, \tag{27}$$

где $\frac{\theta}{12N}\log e=O\left(\frac{1}{N}\right)=o(1)$.

Оценим сумму $\sum_{k=1}^{n} E\log\xi_k!$ Применяя формулу (26), получаем

$$E\log\xi_k! = \sum_{S=0}^{N} \log S! C_N^S P_K^S (1-P_K)^{N-S} = \sum_{S=0}^{N} S\log S \cdot C_N^S P_K^S (1-P_K)^{N-S} + \frac{1}{2}\sum_{S=1}^{N} \log S \cdot C_N^S P_K^S (1-P_K)^{N-S} -$$

$$-\log e \sum_{S=0}^{N} S\, C_N^S P_K^S (1-P_K)^{N-S} + \log\sqrt{2\pi} + \frac{\theta\log e}{12}\sum_{S=1}^{N}\frac{1}{S} C_N^S P_K^S (1-P_K)^{N-S}. \quad (28)$$

Для первой суммы в (28) имеем:

$$\sum_{S=0}^{N} S\log S \cdot C_N^S P_K^S (1-P_K)^{N-S} = NB_N(P_K) + NP_K \log N, \quad (29)$$

где $B_{N(}P_K) = \sum_{S=0}^{N} \frac{S}{N}\log\frac{S}{N} C_N^S P_K^S (1-P_K)^{N-S}$.

Заметим, что функция $U(x) = x\cdot\log x$ непрерывна на отрезке [0,1] и имеет конечную производную 2-го порядка в точке $x = P_k > 0$.

Тогда, применяя теорему о порядке приближения с помощью полиномов Бернштейна [6], получаем

$$B_N(P_k) = U(P_k) + \frac{U''(x)|x=P_k}{2N} P_k(1-P_k) + \frac{\rho_N(k)}{N},$$

где $\rho_N(k) \to 0$ при $N \to \infty$ равномерно по $k = 1,...,n$.

Отсюда, определив $U''(x)|x = P_k$, получаем

$$\sum_{S=0}^{N} S\log S \cdot C_N^S P_K^S (1-P_K)^{N-S} = NP_K \log NP_K + \frac{(1-P_K)\log e}{2} + \rho_N(K), \quad (30)$$

где $\rho_N(k) \to 0$ при $N \to \infty$.

Далее с учетом (24) получаем

$$\sum_{K=1}^{n}\sum_{S=0}^{N} S\log S \cdot C_N^S P_K{}^S (1-P_K)^{N-S} = N\log N - NH_P + (\frac{n-1}{2})\log e + \rho'_N(K), \quad (31)$$

где $\rho'_N(K) = \sum_{K=1}^{n} \rho_N(K) \le n\max_K \rho_N(K) \to 0$ при $N \to \infty$.

Вторую и четвертую сумму в правой части (28) оценим с помощью неравенства Чебышева [7], положив $\varepsilon = N^{\frac{2}{3}} P_K^{\frac{1}{2}}$ и разбив область суммирования по S на 2 части:

$$(S - NP_K) \ge N^{\frac{2}{3}} P_K^{\frac{1}{2}} \quad \text{и} \quad (S - NP_K) < N^{\frac{2}{3}} P_K^{\frac{1}{2}}.$$

Для второй суммы в правой части (28) имеем

$$\sum_{S=1}^{N} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} = \sum_{|S-NP_K| \ge N^{\frac{2}{3}} P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} + \sum_{|S-NP_K| < N^{\frac{2}{3}} P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S}. \quad (32)$$

Для первой суммы в (32) с учетом (23) имеем

$$\sum_{|S-NP_K| \ge N^{\frac{2}{3}} P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} \le (\log N) P\{|\xi_K - NP_K| \ge N^{\frac{2}{3}} P_K^{\frac{1}{2}}\} \le N^{-1/3}(1-P_K)\log N = O(N^{-1/3}\log N) \to 0. \quad (33)$$

при $N \to \infty$.

Для второй суммы в (32) справедливы неравенства:

$$\log(NP_K - N^{\frac{2}{3}}P_K^{\frac{1}{2}})(1-\frac{1-P_K}{N^{\frac{1}{3}}}) \le \sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} \le \log(NP_K + N^{\frac{2}{3}}P_K^{\frac{1}{2}}),$$

или при $N \to \infty$:

$$\log NP_K - o(1) \le \sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} \le \log NP_K + o(1). \quad (34)$$

На основании (33) и (34) имеем асимптотическое равенство

$$\sum_{S=0}^{N} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} = \log NP_K + o(1). \quad (35)$$

Отсюда при условии $N \to \infty$ получаем

$$\frac{1}{2}\sum_{K=1}^{n}\sum_{S=0}^{N} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} = \frac{n}{2}\log N + \frac{1}{2}\sum_{K=1}^{n} \log P_K + o(1). \quad (36)$$

Вычислим четвертую сумму в правой части (28):

$$\sum_{S=1}^{N} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} = \sum_{|S-NP_K|\ge N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} + \sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S}, \quad (37)$$

откуда при условии $N \to \infty$ получаем

$$\sum_{|S-NP_K|\ge N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} \le P\{|\xi_K - NP_K| \ge N^{\frac{2}{3}}P_K^{\frac{1}{2}}\} \le \frac{(1-P_K)}{N^{\frac{1}{3}}} = O(N^{-1/3}) \to 0$$

при условии $N \to \infty$, а для второй суммы в (37) имеет место неравенство

$$(NP_K + N^{\frac{2}{3}}P_K^{\frac{1}{2}})^{-1}(1-\frac{(1-P_K)}{N^{\frac{1}{3}}}) \le \sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^K P_K{}^S (1-P_K)^{N-S} \le (NP_K - N^{\frac{2}{3}}P_K^{\frac{1}{2}})^{-1},$$

откуда следует, что

$$\sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} = O(N^{-1}). \quad (38)$$

Из (37)–(38) следует, что при $N \to \infty$

$$\frac{\theta \log e}{12}\sum_{S=1}^{N} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} = O(N^{-1}),$$

откуда

$$\frac{\theta \log e}{12}\sum_{K=1}^{n}\sum_{S=0}^{N} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} = o(1). \quad (39)$$

Третья сумма в правой части (28) равна:

$$(\log e)\sum_{S=0}^{N} S C_N^S P_K{}^S (1-P_K)^{N-S} = NP_K \log e,$$

откуда,

$$\log e \sum_{K=1}^{n}\sum_{S=0}^{N} S C_N^S P_K{}^S (1-P_K)^{N-S} = N \log e. \quad (40)$$

С учетом (28), (31), (36)−(40) получаем асимптотическое выражение для суммы $\sum_{K=1}^{n} E\log\xi_K!$ при условии $P_k = \text{const}$, $k = 1, \ldots, n$:

$$\sum_{K=1}^{n} E\log\xi_K ! = N\log N - N(H_P + \log e) + \frac{n}{2}\log N + \frac{1}{2}\sum_{K=1}^{n}\log P_K + n\log\sqrt{2\pi} + + \frac{n-1}{2}\log e + o(1). \quad (41)$$

Из (25), (27) и (41) получаем асимптотическое выражение для энтропии полиноминальной схемы $H_N(p_1,...,p_n)$:

$$H_N(p_1,...,p_n) = \frac{n-1}{2}\log N + \frac{1}{2}\sum_{K=1}^{n}\log P_K + \frac{n-1}{2}\log 2\pi e + o(1). \quad (42)$$

Окончательно для взаимной информации $I(M^N, E^N)$ получаем асимптотическое равенство:

$$I(M^N, E^N) = \frac{n-1}{2}\log_2 N - \frac{1}{2}\sum_{k=1}^{n}\log_2 P_k - \frac{n-1}{2}\log_2 2\pi e + o(1), \quad (43)$$

справедливое при условии $N \to \infty$, n=const, $P_k = \text{const}$, k=1,…, n.

Выражения (14) и (43) позволяют оценить значения параметров, в частности длину выходного сообщения N, при котором обеспечиваются важные криптографические качества рассматриваемых преобразований.

Литература

1. Алферов А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. − М.: Гелиос АРВ, 2001. − 479 с.

2. Бабаш А.В. Криптография / А.В. Бабаш, Г.П. Шанкин.− М.: СОЛОН-ПРЕСС, 2007. − 512 с.

3. Колесник В.Д. Курс теории информации / В.Д. Колесник, Г.Ш. Полтырев. − М.: Наука, 1982. − 416 с.

4. Духин А.А. Теория информации. − М.: Гелиос АРВ, 2009. − 248 с.

5. Сачков В.Н. Комбинаторные методы дискретной математики. − М.: Наука, 1966. − 384 с.

6. Березин И.С. Методы вычислений / И.С. Березин, Н.П. Жидков. − 3-е изд. − М.: Наука, 1966. − Т. 1. − 632 с.

7. Боровков А.А. Теория вероятностей. − 2-е изд. − М.: Наука, 1986. − 656 с.

Лось Алексей Борисович
Канд. техн. наук, доцент каф. компьютерной безопасности
Московского института электроники и математики
Национального исследовательского университета «Высшая школа экономики»
Тел.: 8-910-477-88-27
Эл. почта: alos@hse.ru

Los A.B.

The study of information characteristics transformations substitution and permutation

In the paper the results of the research information characteristics of conversion substitution and permutation, which is the basis for building cryptographic algorithms. The obtained value of the mutual information of the input and output messages of discrete communication channel in the application of these reforms.
Keywords: channel, mutual information, conversion substitution and permutation.