ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 45 2009 Вып. 2

УДК 621.391.7

© 2009 г. **Б.Я. Рябко, Д.Б. Рябко**

АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫЕ СОВЕРШЕННЫЕ СТЕГАНОГРАФИЧЕСКИЕ СИСТЕМЫ[1]

В 1998 году Кашен (Cachin) предложил теоретико-информационный подход к стеганографии, в рамках которого, в частности, была определена так называемая совершенная стегосистема, у которой сообщения, несущие и не несущие скрытую информацию, статистически неразличимы. Там же была описана и универсальная стеганографическая система, для которой это свойство выполняется только асимптотически, при увеличении длины сообщения, причем сложность кодирования и декодирования возрастает экспоненциально. (По определению система универсальна, если она применима и в том случае, когда вероятностные характеристики сообщений, которые используются для передачи скрытой информации, известны не полностью.)

В данной статье предлагается универсальная стеганографическая система, у которой сообщения, несущие и не несущие скрытую информацию, статистически неразличимы, и при этом скорость передачи "скрытой" информации приближается к пределу – энтропии Шеннона источника, используемого для "встраивания" скрытой информации.

§ 1. Введение

Стеганографические системы передачи информации предназначены для "скрытой" передачи сообщений, "спрятанных" в открыто передаваемых данных (таких как письма, цифровые фотографии, фильмы и т.п.). Другими словами, целью стеганографии является передача защищенных от несанкционированного доступа (например, зашифрованных) данных таким образом, что сам факт передачи остается скрытым. Это условие формулируется следующим образом: сообщения, несущие и не несущие скрытую информацию, должны подчиняться одному и тому же распределению вероятностей, и следовательно, быть статистически неразличимыми [1].

Во многих случаях использования стегосистем закон распределения вероятностей сообщений, в которые "встраивается" скрытая информация, точно не известен, а в случае, когда эти сообщения суть цифровые фотографии, фильмы, музыкальные произведения, электронные письма, SMS- и ICQ-сообщения и т.п., закон распределения, по-видимому, и не может быть известен точно. Поэтому довольно естественной кажется рассмотренная в [1] задача построения так называемых универсальных стегосистем, в которых закон распределения вероятностей сообщений, в которые "встраивается" скрытая информация, не известен, но априори известно, что порождаемые источником символы одинаково распределены и независимы.

Приведем некоторые обозначения, используемые в дальнейшем. Мы будем считать, что дан некоторый источник *открытых сообщений* μ, порождающий независимые и одинаково распределенные случайные величины, принимающие значения

[1] Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 06-07-89025).

из некоторого (возможно, бесконечного) алфавита A. Есть два участника – Алиса и Боб, и Алиса собирается использовать этот источник для скрытой передачи сообщений, состоящих из последовательности символов из алфавита $B = \{0, 1\}$, порождаемых независимо и с равными вероятностями. Этот источник мы обозначим через ω и в дальнейшем будем называть его *источником секретных сообщений*. Такая модель источника секретных сообщений является фактически общепринятой, так как обычно предполагается, что секретные сообщения уже зашифрованы Алисой с ключом, известным только ей и Бобу. Если Алиса использует шифр Вернама, то зашифрованная последовательность состоит из равновероятных и независимых символов; если же используются современные блоковые или потоковые шифры с секретным ключом, то зашифрованная последовательность должна быть "похожа" на цепочку равновероятных и независимых двоичных символов. ("Похожесть" может означать неотличимость за полиномиальное время или подтверждаться экспериментальными статистическими данными, имеющимися для всех современных шифров; подробнее см., например, [2,3].) Кроме Алисы и Боба, есть еще один участник – Ева, который читает все сообщения, передаваемые от Алисы к Бобу и пытается установить, не содержат ли сообщения какую-либо скрытую информацию. Заметим сразу, что если сообщения, содержащие и не содержащие встроенную секретную информацию, подчиняются одному и тому же закону распределения вероятностей, то Ева (и никто другой) не может различать такие сообщения. Благодаря этому свойству такие системы в [1] названы совершенными.

Для описанной нами модели в [1] предложена конструкция универсальной стегосистемы, в которой последовательность символов, порождаемая источником секретных сообщений, разбивается на подслова (блоки) некоторой длины m, каждому из которых ставится в соответствие определенное слово фиксированной длины $n(m)$ из алфавита A, так что при этом последовательность получаемых символов подчиняется распределению вероятностей, приближающемуся к (неизвестному) μ. (Напомним, что распределению μ подчиняются сообщения, не содержащие скрытой секретной информации.) Важно отметить, что, во-первых, хотя распределение вероятностей сообщений стегосистемы сходится к распределению μ при увеличении длины сообщений n, эта сходимость не равномерная (относительно множества всех вероятностных распределений μ при фиксированном алфавите A), и во-вторых, объем памяти кодера и декодера данной стегосистемы возрастает экспоненциально при увеличении n. По этим двум причинам стегосистема из [1] является практически не применимой. В работах [4, 5] подход и результаты Кашена [1] использовались для построения и анализа стегосистем, которые в том или ином смысле близки к совершенным, но не совершенны.

В данной статье впервые предлагается конструкция универсальной стегосистемы, лишенная недостатков метода из [1]: у нее сообщения, несущие и не несущие скрытую информацию, статистически неразличимы при любой длине сообщения, т.е. она является совершенной. Кроме того, показано, что скорость передачи скрытой информации ограничена предельной величиной – энтропией Шеннона источника μ, и найдены конструкции стегосистем, где эта скорость приближается к пределу. Важно отметить, что предлагается простой алгоритм кодирования и декодирования, сложность которого растет полиномиально при стремлении скорости передачи спрятанной информации к ее пределу – энтропии Шеннона.

§ 2. Простейшая универсальная стегосистема

Для того чтобы объяснить основную идею предлагаемой конструкции, мы начнем описание системы с простейшего случая, когда не только источник секретных символов ω двоичный, но и источник открытых сообщений μ порождает последовательность независимых символов из двоичного алфавита $A = \{a, b\}$. Пусть требуется

передавать (секретную) последовательность символов $y^* = y_1y_2y_3\ldots$, порождаемую источником независимых и равновероятных двоичных символов ω, и пусть имеется последовательность символов $x^* = x_1x_2x_3\ldots$, порожденная μ. Например, пусть

$$y^* = 0110\ldots, \quad x^* = aababaaaabbaaaaabb\ldots \tag{1}$$

При кодировании последовательности x^* и y^* преобразуются в новую последовательность X, передаваемую Бобу, такую что, во-первых, по X Боб может однозначно восстановить (секретную) последовательность y^*, и во-вторых, распределение вероятностей символов в X такое же, как и в x^*. (Другими словами, X и x^* статистически неразличимы.) Процесс построения последовательности X по x^* и y^* мы разобьем на этапы. Сначала разделим все символы X^* на пары, и для удобства обозначим все возможные пары следующим образом:

$$aa = u, \quad bb = u, \quad ab = v_0, \quad ba = v_1.$$

Например, последовательность из (1) можно представить в виде

$$x^* = aa\,ba\,ba\,aa\,ab\,ba\,aa\,aa\,bb\ldots = uv_1v_1uv_0v_1uuu\ldots$$

(пробелы поставлены только для удобства чтения). Затем сформируем последовательность X следующим образом: все пары букв, соответствующие u, оставим без изменения, а пары, соответствующие v_k, заменим последовательно на пары букв, соответствующие $v_{y_1}v_{y_2}v_{y_3}\ldots$ В рассматриваемом примере (1) мы получим следующую последовательность X:

$$X = aa\,ab\,ba\,aa\,ba\,ab\,aa\,aa\,bb\ldots$$

Декодирование очевидно: Боб разбивает полученную последовательность символов X на пары и заменяет пары ab и ba на 0 и 1 соответственно, а остальные пары символов просто пропускает.

Свойства описанного метода, который мы обозначим через St_2, характеризует следующий почти очевидный факт.

Утверждение. *Пусть дан источник μ, порождающий независимые и одинаково распределенные случайные величины, принимающие значения из алфавита $A = \{a, b\}$, и пусть этот источник используется для скрытой передачи сообщений, состоящих из независимых и равновероятных двоичных символов, по описанному методу St_2.*

Тогда распределение вероятностей сообщений, получаемых на выходе стегосистемы, то же, что и у источника μ.

Мы не будем приводить вполне очевидное доказательство этого утверждения, так как оно является частным случаем приводимой ниже теоремы 1.

Интересно отметить, что близкая конструкция была использована фон Нейманом при построении последовательности равновероятных двоичных символов (см. [6, 7]). Его метод, как и описанная стегосистема, базировался на том, что вероятности появления пар символов ab и ba равны.

Описанную выше конструкцию легко обобщить на случай произвольного алфавита A. Действительно, зададим на множестве всех букв A какой-либо порядок. (Здесь стоит отметить, что A может состоять из графических файлов или фотографий, но в любом случае все эти и подобные объекты представлены в системах передачи информации в виде двоичных слов и могут быть упорядочены, скажем, лексикографически.) Как и ранее, для того чтобы передать (секретную) последовательность символов $y^* = y_1y_2y_3\ldots$, порождаемую источником независимых и равновероятных двоичных символов ω, имеющаяся последовательность символов $x^* = x_1x_2x_3\ldots$,

порожденная источником независимых символов μ, $x_i \in A$, разбивается на блоки длины 2. Если блок $x_{2i-1}x_{2i}$ состоит из одинаковых букв, то он не используется для кодирования и передается без изменений; если же блок $x_{2i-1}x_{2i}$ состоит из разных букв, скажем, α и β, то он используется для кодирования очередного символа, который мы обозначим через y_k. Без ограничения общности предположим, что $\alpha < \beta$ при заданном упорядочивании; тогда в передаваемую последовательность включается слово $\alpha\beta$, если $y_k = 0$, и слово $\beta\alpha$, если $y_k = 1$. Декодирование очевидно: если пара символов $X_{2i-1}X_{2i}$ в закодированной последовательности состоит из одинаковых букв, то она не кодирует символ из $y^* = y_1y_2y_3\ldots$ Если же $X_{2i-1}X_{2i}$ различны и $X_{2i-1} < X_{2i}$ (при заданном упорядочивании), то очередной скрыто передаваемый символ y_k равен 0, в противном случае $y_k = 1$. Обозначим описанную стегосистему через $\mathrm{St}_2(A)$.

Теорема 1. *Пусть дан источник μ, порождающий независимые и одинаково распределенные случайные величины, принимающие значения из некоторого алфавита A, и пусть этот источник используется для скрытой передачи сообщений, состоящих из независимых и равновероятных двоичных символов с помощью стегосистемы $\mathrm{St}_2(A)$. Тогда распределение вероятностей сообщений, получаемых на выходе стегосистемы, то же, что и у источника μ, а среднее количество передаваемых букв, приходящихся на один секретно передаваемый бит, равно $2/\Big(1 - \sum\limits_{a\in A} \mu(a)^2\Big)$.*

Доказательство. Возьмем произвольные $\alpha, \beta \in A$ и i и покажем, что

$$P(X_{2i-1}X_{2i} = \alpha\beta) = \mu(\alpha\beta).$$

Если $\alpha = \beta$, то $P(X_{2i-1}X_{2i}) = P(x_{2i-1}x_{2i})$, т.е. вероятности в последовательности, содержащей скрытую информацию, и в исходной совпадают. Пусть теперь $\alpha < \beta$. Тогда

$$P(X_{2i-1}X_{2i} = \alpha\beta) = P(y_k = 0)P(x_{2i}x_{2i+1} = \alpha\beta) + P(y_k = 0)P(x_{2i}x_{2i+1} = \beta\alpha) =$$
$$= 1/2\mu(\alpha)\mu(\beta) + 1/2\mu(\beta)\mu(\alpha) = \mu(\alpha)\mu(\beta).$$

Случай $\beta > \alpha$ разбирается аналогично. Второе утверждение получается прямым вычислением вероятности того, что в блоке обе буквы одинаковы. ▲

Отметим, что на практике, когда открыто передаваемые символы из A являются, например, графическими файлами и каждый файл практически уникален, алфавит A огромен, так что среднее количество передаваемых букв (графических файлов), приходящихся на один секретно передаваемый бит, примерно равно двум.

§ 3. Общая конструкция универсальной стегосистемы

Перейдем к описанию общего метода. Пусть, как и ранее, требуется передавать (секретную) последовательность символов $y^* = y_1y_2y_3\ldots$, порождаемую источником независимых и равновероятных двоичных символов ω, и пусть имеется последовательность символов $x^* = x_1x_2x_3\ldots$, порожденная источником независимых символов μ, где каждый символ x_i принадлежит алфавиту A. В предлагаемой стегосистеме последовательность x^* разбивается на блоки длины n, где $n > 1$ – параметр метода.

Каждый блок используется для кодирования некоторого числа символов из y^* (например, в ранее описанной стегосистеме $\mathrm{St}_2(A)$ каждый блок из двух символов кодировал либо одну букву из y^*, либо ноль букв). Однако в общем случае возникает одна особенность, не встречавшаяся в случае двухбуквенного блока. Точнее,

возникает задача согласования вероятностей блоков из последовательностей x^* и y^*. Дело в том, что вероятности слов, порождаемых источником секретных символов, кратны степени числа 2, тогда как количество равновероятных блоков может не удовлетворять этому условию.

Перейдем к точному описанию. Обозначим через u первые n букв из последовательности x^*: $u = x_1 \dots x_n$, и пусть $\nu_u(a)$ – количество букв a в слове u. По определению множество S_u состоит из всех слов длины n, у которых частота встречаемости каждой буквы из алфавита A та же, что и в слове u, т.е. S_u состоит из слов частотного класса слова u. (Для того чтобы пояснить смысл рассмотрения этого множества, заметим, что вероятности всех его элементов равны, так как μ – источник независимых и одинаково распределенных случайных величин.) Пусть на множестве слов S_u задан какой-либо порядок (скажем, лексикографический), известный Алисе и Бобу, и пусть $S_u = \{s_0, s_1, \dots, s_{|S_u|-1}\}$ при этом упорядочивании.

Обозначим $m = \lfloor \log_2 |S_u| \rfloor$, где $\lfloor y \rfloor$ – наибольшее целое, не превосходящее y. Рассмотрим двоичное представление числа $|S_u|$:

$$|S_u| = (\alpha_m, \alpha_{m-1}, \dots, \alpha_0),$$

причем $\alpha_m = 1$, $\alpha_j \in \{0, 1\}$, $m > j \geqslant 0$. Другими словами,

$$|S_u| = \alpha_m 2^m + \alpha_{m-1} 2^{m-1} + \alpha_{m-2} 2^{m-2} + \ldots + \alpha_0, \quad \alpha_m = 1.$$

Обозначим через $\delta(u)$ номер слова u (при заданном на S_u порядке), и пусть $(\lambda_m, \lambda_{m-1}, \dots, \lambda_0)$ – двоичное представление числа $\delta(u)$. Пусть $j(u)$ – наибольшее из чисел, таких что $\alpha_j \neq \lambda_j$. Алиса, определив $j(u)$, считывает $j(u)$ букв из последовательности скрытно передаваемых символов y^*, и пусть эти символы, рассматриваемые как число в двоичной системе счисления, равны τ. Алиса находит в множестве S_u слово v, номер которого в S_u равен $\sum\limits_{j(u)<s\leqslant m} \alpha_s 2^s + \tau$, и передает слово v Бобу (или, другими словами, v помещается в выходную последовательность кодера).

При декодировании Боб, получив слово v, определяет множество S_v (совпадающее с S_u), находит так же, как при кодировании, $j(v)$ (для u и v они совпадают: $j(u) = j(v)$) и τ, а затем по τ определяет $j(v)$ закодированных символов. Все последующие n-буквенные слова кодируются Алисой и декодируются Бобом аналогично. Обозначим эту систему через $\mathrm{St}_n(A)$.

Рассмотрим пример, иллюстрирующий все этапы вычислений. Пусть $A = \{a, b, c\}$, $n = 3$, $u = bac$. Тогда $S_u = \{abc, acb, bac, bca, cab, cba\}$, $|S_u| = 6$, $m = 2$, $\alpha_2 = 1$, $\alpha_1 = 1$, $\alpha_0 = 0$, $\delta(u) = 2$, $\lambda_2\lambda_1\lambda_0 = 010$, $j(u) = 2$. Вычислив эти значения, Алиса считывает $j(u)$ $(= 2)$ секретно передаваемых символов последовательности y^*. Пусть для определенности эти символы равны 11. После этого Алиса находит $j(v) = 2$ и номер слова v в S_v $(= S_u)$, в данном случае равный $\sum\limits_{2<s\leqslant 2} \alpha_s 2^s + \tau = 0 + 3 = 3$. Соответствующим ему словом является $v = bca$. Боб, получив это слово, определяет по нему S_v $(= S_u)$, $\tau = 3$, а по значению τ – переданные секретные символы 11.

Т е о р е м а 2. *Пусть дан источник μ, порождающий независимые и одинаково распределенные случайные величины, принимающие значения из некоторого алфавита A, и пусть этот источник используется для скрытой передачи сообщений, состоящих из независимых и равновероятных двоичных символов, по описанному выше методу $\mathrm{St}_n(A)$ при длине блока n, $n \geqslant 2$. Тогда выполнены следующие утверждения*:

(i) *Сообщения, получаемые на выходе стегосистемы, подчиняются распределению μ (т.е. распределения входной и выходной последовательности кодера одинаковые, и следовательно, система совершенна)*;

(ii) *Среднее число L_n скрытых символов на букву источника удовлетворяет неравенству*

$$L_n \geqslant \frac{1}{n}\left(\sum_{u\in A^n}\mu(u)\log\frac{n!}{\prod\limits_{a\in A}\nu_u(a)!}-2\right), \tag{2}$$

где $\mu(u)$ – вероятность порождения слова u источником μ, а $\nu_u(a)$ – количество букв a в слове u.

(iii) *Если алфавит A конечен и длина блока n стремится к бесконечности, то среднее число L_n скрытых символов на букву стремится к энтропии Шеннона источника сообщений $h(\mu)=-\sum\limits_{a\in A}\mu(a)\log\mu(a)$.*

Доказательство. Для доказательства утверждения (i) теоремы достаточно показать, что для каждого n-буквенного слова u из входной (исходной) последовательности вероятность появления в кодирующей последовательности любого слова $v\in S_u$ равна $1/|S_u|$. Доказательство, как и ранее, основано на применении формулы полной вероятности. Как видно из описания, вероятность того, что из последовательности скрытно передаваемых символов будет считано j, $j=0,\dots,m$, равна $2^j/|S_u|$, если $\alpha_j=1$ (так как номер слова u в S_u должен удовлетворять неравенству $\sum\limits_{j(u)<s\leqslant m}\alpha_s 2^s \leqslant \delta(u) < \sum\limits_{j(u)\leqslant s\leqslant m}\alpha_s 2^s$). Пусть для определенности u и v – первые слова в исходной и закодированной последовательностях. Тогда

$$P(X_1\dots X_n=v)=P\big(u\in S_v \text{ и } j(v)=j(u)\big)2^{-j(v)}.$$

Здесь последний множитель равен вероятности считать из последовательности секретно передаваемых символов y^* двоичное слово длинны $j(v)$, кодирующее v. Из последнего равенства получаем

$$\begin{aligned}&P(X_1\dots X_n=v)=P(u\in S_v)P\big(j(v)=j(u)\,|\,u\in S_v\big)2^{-j(v)}=\\&=|S_v|\mu(u)\big(2^{j(v)}/|S_v|\big)2^{-j(v)}=\mu(u).\end{aligned}$$

Так как u и v принадлежат одному частотному классу, из последнего равенства видно, что $P(X_1\dots X_n=v)=\mu(v)$.

Для доказательства утверждения (ii) определим величину $\phi=2^m/|S_u|$ и обозначим через $L(S_u)$ среднее число скрытно передаваемых символов, приходящихся на одно слово из S_u:

$$L(S_u)=\frac{1}{|S_u|}\sum_{i=0}^{m}\alpha_i i 2^i.$$

Справедливы следующие соотношения:

$$\begin{aligned}&L(S_u)=\frac{1}{|S_u|}\sum_{i=0}^{m}\alpha_i i 2^i=\frac{1}{|S_u|}\left(m\sum_{i=0}^{m}\alpha_i 2^i-\sum_{i=0}^{m}\alpha_i 2^i(m-i)\right)=\\&=m-\left(2^m\sum_{k=0}^{m}k\alpha_{m-k}2^{-k}\right)>m-2^{m+1}/|S_u|=m-2/\phi=\\&=\log|S_u|-\log\phi-2/\phi.\end{aligned}$$

Можно проверить прямым нахождением максимума, что $\log\phi+2/\phi\leqslant 2$ при $\phi\in[1,2]$. Из этого получаем, что $L(S_u)>\log|S_u|-2$. Отсюда и из равенства $|S_u|=\dfrac{n!}{\prod\limits_{a\in A}\nu_u(a)!}$ получаем утверждение (ii) теоремы.

Утверждение (iii) следует из широко известного в теории информации факта о том, что с вероятностью, стремящейся к единице, справедливо неравенство $h(\mu)-\delta < \log|S_u|/n < h(\mu)+\delta$ при любом $\delta > 0$ (см., например, [8, 9]). ▲

Во многих реальных стегосистемах алфавит A огромен (скажем, состоит из всех возможных цифровых фотографий заданного формата или всех возможных электронных писем). В этом случае представляет интерес асимптотическое поведение L_n при фиксированном n и $|A| \to \infty$. Для точного рассмотрения этого случая мы будем использовать понятие минимум-энтропии (minimum entropy или minentropy), которое определяется равенством

$$H_\infty(\mu) = \min_{a \in A}\{-\log \mu(a)\}. \tag{3}$$

Следствие. *Если выполнены условия теоремы, длина блока n конечна и количество букв в алфавите A стремится к бесконечности так, что $H_\infty(\mu) \to \infty$, то величина L_n удовлетворяет неравенствам*

$$\log(n!)/n \geqslant L_n \geqslant (\log(n!) - 2)/n,$$

что при больших n эквивалентно асимптотическому равенству

$$L_n = \log n(1 + o(n)).$$

Это утверждение легко выводится из того, что число перестановок из n различных элементов равно $n!$ и утверждения (ii) теоремы 2.

Остановимся теперь кратко на оценке сложности стегосистемы $\mathrm{St}_n(A)$. Хранение всех слов из множества S_u потребовало бы порядка $2^n \log|A|$ бит памяти, что, конечно, практически нереализуемо при больших n. В [10] предложен алгоритм быстрой нумерации, который позволяет находить номер блока любого слова u в множестве S_u при кодировании и проводить обратную операцию при декодировании, затрачивая $O(\log^{\mathrm{const}} n)$ операций на символ при объеме памяти $O(n \log^3 n)$ бит.

Стоит отметить, что основная идея, использованная при построении стегосистемы $\mathrm{St}_n(A)$, применима и к более общим источникам открытых сообщений, чем источники, порождающие независимые одинаково распределенные сообщения. В самом деле, единственное свойство таких источников, которое мы использовали, заключается в том, что все блоки сообщений, полученные друг из друга перестановками, имеют одинаковую вероятность. Если источник открытых сообщений обладает тем свойством, что на каком-то шаге некоторые сообщения имеют одинаковую (условную) вероятность, то в случае генерации источником одного из этих сообщений, заменяя его при необходимости на одно из равновероятных, можно передать секретную информацию. Сообщения, не принадлежащие ни одной группе равновероятных сообщений, для кодирования секретной информации не используются. Источники, порождающие независимые одинаково распределенные сообщения, – всего лишь один простой и содержательный пример кодирования такого рода.

Авторы выражают глубокую благодарность Г.А. Кабатянскому, предложившему существенное упрощение описанного в статье метода и простое доказательство оценки в теореме 2.

СПИСОК ЛИТЕРАТУРЫ

1. *Cachin C.* An Information-Theoretic Model for Steganography // Proc. 2nd Int. Workshop on Information Hiding. Lecture Notes Comput. Sci. V. 1525. Berlin: Springer, 1998. P. 306–318.
2. *Рябко Б.Я., Фионов А.Н.* Криптографические методы защиты информации. М.: Телеком, 2005.

3. *Menzes A., van Oorschot P., Vanstone S.* Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996.
4. *Salle P.* Model-Based Steganography // Proc. 2nd Int. Workshop on Digital Watermarking. Lecture Notes Comput. Sci. V. 2939. Berlin: Springer, 2004. P. 154–167.
5. *Mittelholzer T.* An Information-Theoretic Approach to Steganography and Watermarking // Proc. 3rd Int. Workshop on Information Hiding. Lecture Notes Comput. Sci. V. 1768. Berlin: Springer, 1999. P. 1–16.
6. *von Neumann J.* Various Techniques Used in Connection with Random Digits // Monte Carlo Methods. Applied Mathematics Series. № 12. Washington: U.S. National Bureau of Standarts. 1951. P. 36–38.
7. *Elias P.* The Efficient Construction of an Unbiased Random Sequence // Ann. Math. Statist. 1972. V. 43. № 3. P. 865–870.
8. *Csiszar I.* The Method of Types // IEEE Trans. Inform. Theory. 1998. V. 44. № 6. P. 2505–2523.
9. *Галлагер Р.* Теория информации и надежная связь. М.: Сов. радио, 1974.
10. *Рябко Б.Я.* Быстрая нумерация комбинаторных объектов // Дискретная математика. 1998. Т. 10. № 2. С. 101–119.

Рябко Борис Яковлевич
Сибирский государственный университет
телекоммуникаций и информатики
Институт вычислительных технологий СО РАН
boris@ryabko.net
Рябко Даниил Борисович
ИНРИА, Лилль, Франция
daniil@ryabko.net

Поступила в редакцию
09.02.2006
После переработки
23.02.2009