ГЕНЕРИРОВАНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ (ППСЧ) МЕТОДОМ КОМБИНАТОРНЫХ ПЕРЕСТАНОВОК ДИСКРЕТНОЙ ДВУМЕРНОЙ ИНФОРМАЦИИ

Бурцев Вал.Н., Бурцев Влад.Н., Ерохин А.Л.
Харьков, Украина

В автоматизированных системах обработки информации (АСОИ) безопасность защиты баз данных от несанкционированного проникновения осуществляется аппаратно-программными комплексами шифрования [1÷3]. Блок генерации ППСЧ является одной из их частей. Основными способами генерации являются компьютерные программы конгруэнтного генератора [3. стр. 75] и вычисления рекуррентных соотношений с их разностными уравнениями [4]. Конгруэнтные генераторы строят ППСЧ с длиной периода 2^{24}, что является недостаточным для обеспечения криптостойкости шифросистем. Вычисления рекуррентных отношений увеличивают период до значения $(2^m - 1)$ [4]. Все применяемые криптосистемы формально представляют собой однопараметрическое семейство обратимых функций преобразований.

$$(E)_{k\in\bar{k}} : \overline{M} \to \overline{C} \qquad (1)$$

$$(D)_{k'\in\bar{k}} : \overline{C} \to A \qquad (2)$$

где $(E)_{k\in\bar{k}}$ и $(D)_{k'\in\bar{k}}$ прямые и обратные преобразования шифрования-расшифрования;

$(\overline{M})$ - пространство открытых текстов, переводимых преобразованием (E)

в пространство зашифрованных текстов $(\overline{C})$;

$\bar{k}$ - пространство параметров ключей шифрования-расшифрования;

Преобразования (E) и (D) являются обратимыми

$$(E)_{k\in\bar{k}} * (D)_{k'\in\bar{k}} = 1 \qquad (3)$$

Следует отметить, что все применяемые программы на самом деле выдают детерминированные числовые последовательности, по своим свойствам похожие на случайные [5].

Определенный интерес для криптографии могут представлять оптические генераторы ППСЧ с волоконно-оптическими преобразователями информации (ВОПИ) [6,7] , посредством которых удается моделировать марковские процессы [8,9]. Первые сведения о кодировании волоконно-оптическими системами были приведены в [10], где световоды произвольным образом «перепутаны» (с реализацией симметричных криптосистем шифрования-расшифрования двумерной информации). Для этого способа есть ряд трудностей, присущих симметричным криптосистемам. Более перспективным может считаться использование ВОПИ в качестве генератора ППСЧ.

Достоинством любой волоконно-оптической системы является ее способность преобразовывать любую континуальнозаданную двумерную информацию в виде объединения дискретных фрагментов ее, заданных матрицами [8,9].

$$(A,F) = \sum_{i=1}^{m}\sum_{j=1}^{n}(a_{ij})^{f_{ij}} \qquad (4)$$

где *F* – информация, исходно заданная в континуальном пространстве

fij – дискретные фрагменты информации *F(x,y),* заданные на носителях *aij*, являющихся поперечными сечениями световодов.

Определим базовую систему координат носителей *aij є A*:

$$a1,j \quad j = 1, 2, \ldots n$$
$$ai,1 \quad i = 1, 2, \ldots M \qquad (5)$$

Введем в рассмотрение предикат «совпадения-несовпадения координат взаимных положений фрагмента fkl на носителе aij , в базисе (5). Указанные предикаты имеют значения

$P(f_{ij})=(a_{ij}^{f_{ij}})=1$, при совпадении координат (6)

$P(f_{ke})=(a_{ij}^{f_{ke}})=0$, при несовпадении координат

В системе (5) все предикаты *aij*=1 и матрица (4) представляются в виде квантора существования

$$(A,F)=\exists=\begin{pmatrix}1&1&1&.&.&.&1\\1&1&1&.&.&.&1\\.&.&.&.&.&.&.\\1&1&1&.&.&.&1\end{pmatrix} \quad (7)$$

Преобразования комбинаторного типа в ВОПИ осуществляются произвольными перестановками световодов на его выходе относительно сопряженных им сечениям на входе (A, F). В свою очередь множество перестановок образуют матрицу

$$(B,F')=\sum_{i=1}^{m}\sum_{j=1}^{n}b_{ij}^{\,f_{kl}} \quad (8)$$

где F' –закодированная информация в виде компактного набора дискретных фрагментов *fkl*, заданных на носителях *bij.*

Рассмотрим предикаты ($b_{ij}^{\,f_{kl}}$) «совпадения координат положения носителя *bij* и фрагмента *fkl* », которые по аналогии с (6), также принимают значения 0 и 1. Для системы координат

$$a1,j\ \ j=1,2,\ldots.\ n$$
$$ai,1\ \ i=1,2,\ldots.m \quad (9)$$

Матрица (8) также представима квантором существования (7).

В общем виде перестановки световодов в ВОПИ являются системой отношений между носителями *aij* и сопряженными *bkl*, которое предоставимо некоторым прямым (K) и обратным ($\overline{K}$) преобразованиями

$$(K):(A,F')\to(B,F');(\overline{K}):(B,F')\to(A,F) \quad (10)$$

$$(K)*(\overline{K})=1 \quad (11)$$

В систему отношений (10) введем предикаты «совпадения-несовпадения координат носителей *aij* и *bkl* ». Тогда преобразования (K) и ($\overline{K}$) также представимы в виде матриц:

$$(K)=\sum_{i=1}^{m}\sum_{j=1}^{n}(a_{ij})^{b_{kl}} \quad (12)$$

$$(\overline{K})=\sum_{i=1}^{m}\sum_{j=1}^{n}(b_{kl})^{a_{ij}} \quad (13)$$

В соответствии со значениями предикатов $a_{ij}^{\,b_{kl}}$ строки или столбцы матриц (12,13) состоят из последовательностей элементов 0 и 1. В ВОПИносители *aij* и *bkl* фиксированы, поэтому структура элементов «0» и «1» является инвариантной, не зависимой от положения ВОПИ. Прямой и обратный матричные инварианты (12,13) являются своеобразным «паспортом» каждого ВОПИ и технология их изготовления не позволяет принципиально создать два одинаковых кодирующих (декодирующих) преобразователя. При вращении ВОПИ вокруг оси матрицы (12,13) образуют конечную последовательность матриц переходных состояний системы «исходная информация – ВОПИ». В качестве источника информации, генерирующей после преобразования ППСЧ, используются регулярные контрастные штрихи или решетки, относительно которых вращается входной торец ВОПИ. Введем угловой параметр поворота $0 \le \varphi \le 2\pi$ базовых систем координат (5,9). Тогда однопараметрическое семейство преобразований

$$(K)_\varphi:(A,F)_\varphi\to(B,F')_\varphi \quad (14)$$

$$(\overline{K})_\varphi:(B,F')_\varphi\to(A,F')_\varphi \quad (15)$$

Образуют множество матриц переходных состояний по параметру φ.

Указанные множества являются элементами генерации ППСЧ.

Последовательность генерируется при сканировании «строки» («столбца») любой из матриц семейств (14) прямых и (15) обратных преобразований. Используются две схемы сканирования, первая из которых – меридиональная, генерирует последовательности, расположенные на большом диаметре ВОПИ с цилиндрической формой торцов. Число малых последовательностей равно числу углового параметра $0 \le \varphi \le 2\pi$, умноженному на число элементарных световодов, расположенных на этом диаметре. Вторая схема – сагитальное сканирование по любой из хорд торца ВОПИ, включая и диаметр его. Число малых

последовательностей определяется полным перебором угловых положений ВОПИ, имеющих переменное число элементов «0» и «1». Полный период ППСЧ составляет

$$Tc = Rt1 + Rt2 + \ldots + Rtn \approx R\,(m+n) \qquad (16)$$

где R – число угловых положений ВОПИ;

ti- период малой последовательности элементов «0» и «1»;

(m x n)- общее число световодов, образующих ВОПИ;

Для ВОПИ диаметром 20 мм и диаметром световодов – 0.02 мм, число световодов - $7.5*10^5$, число поворотов ВОПИ – 2160, длина периода ППСЧ при меридиональном сканировании составляет не менее 2^{21}, при сагитальном – период $Tc \geq 2^{30}$.

Выводы:

- ВОПИ дают возможность генерировать недетерминированные ППСЧ, сопряженные друг другу.
- Все ВОПИ обладают собственными матричными инвариантами прямого и обратного преобразований, дающие возможность генерации гаммы ключей для асимметричных систем шифрования-расшифрования.

Литература:

1. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

2. Месси Дж. Л. Введение в современную криптологию //ТИИЭР. 1979. Т. 67 №3 С. 71-109;

3. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь. 1999. 328 с.;

4. Диффи У., Хеллман М. Э. Защищенность и имитостойкость. Введение в криптографию. //ТИИЭР. 1979. Т. 67 №3 С. 71-109;

5. Жельников В. Криптография от папируса до компьютера. М.: АВГ. 1979. 336 с.;

6. Бурцев В. Н., Бурцев Вл. Н. Устройство формирования цветовых изображений. Патент России № 1320585, 1996;

7. Бурцев В. Н., Бурцев Вл. Н. Волоконно-оптические преобразователи изображений. Патент России № 2124747, 1999;

8. Бурцев В. Н., Бурцев Вл. Н. Способ моделирования стохастических процессов с помощью комбинаторно-топологических преобразований.// Пробл. Бионики. 2000. Вып. 51. С.

9. Бурцев В. Н., Бурцев Вл. Н., Ерохин А. Исследование стохастических процессов комбинаторно-топологического кодирования информации.// Радиоэлектроника и информатика. 2000. №4 (в печати);

10. Капани Н. Волоконная оптика. Принципы и применение. М.: Мир. №969. 464 с.

GENERATION OF SEQUENCES OF PSEUDORANDOM NUMBERS BY A METHOD OF COMBINATORIAL SWAPS OF THE DISCRETE TWO-DIMENSIONAL INFORMATION

Bourtsev Val.N., Bourtsev Vlad.N., Yerokhin A.L.
Kharkov, Ukraine

All used cryptosystems formally represent an one-parameter family of converted functions of conversions.

$$(E)_{k\in\bar{k}} : \overline{M} \to \overline{C}$$

$$(D)_{k'\in\bar{k}} : \overline{C} \to A$$

Where $(E)_{k\in\bar{k}}$ and $(D)_{k'\in\bar{k}}$ straight linees and reconversions of encoding - расшифрования;

$(\overline{M})$ - space of plain texts translated by conversion (E) In space of the enciphered texts $(\overline{C})$;

$\bar{k}$ - space of parameters of keys of encoding -;

The conversions (E) and (D) are converted

$$(E)_{k\in\bar{k}} * (D)_{k'\in\bar{k}} = 1$$

The defined interest for cryptography can be represented with optical generators with fibre-optical converters (FOC) of the information advantage of any fibre-optical system is its ability to transform anyone the two-dimensional information as association of discrete fragments it, given by matrixes.

$$(A,F) = \sum_{i=1}^{m}\sum_{j=1}^{n}(a_{ij})^{f_{ij}}$$

Where F - information initially given in continual space

fij - discrete fragments of the information F (x, y), given on carriers aij, light-guides, being the cross-sections.

We shall define the kernel system of coordinates of carriers aij є A:

a1, j j = 1, 2, …. n

ai, 1 i = 1, 2, …. M

the conversions of a combinatorial type in FOC are carried out arbitrary swaps of light-guides on its output concerning conjugate by it to cuts on an input (A, F). In turn set of swaps will derivate a matrix

$$(B,F') = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}^{\,f_{kl}}$$

Where F' the encoded information as a compact set of discrete fragments fkl, given on carriers bij.

In a general view of swap of light-guides in FOCявляются by the system of the ratioes between carriers aij and conjugate bkl, which is submitiven to some straight line (K) and converse ($\overline{K}$) by conversions

$$(K):(A,F') \to (B,F');(\overline{K}):(B,F') \to (A,F) \qquad (K)*(\overline{K}) = 1$$

Into the system of the ratioes we shall enter predicates « coincidences - incongruity of coordinates of carriers aij and bkl ». Then conversions (K) and ($\overline{K}$) also present as matrixes:

$$(K) = \sum_{i=1}^{m}\sum_{j=1}^{n}(a_{ij})^{b_{kl}} \qquad (\overline{K}) = \sum_{i=1}^{m}\sum_{j=1}^{n}(b_{kl})^{a_{ij}}$$

According to values of predicates strings or the columns of matrixes consist of sequences of units 0 and 1. The carriers aij and bkl are fixed, therefore structure of units "«0" and "1" is invariant, not dependent from a position FOC. The direct and return matrix invariants are original "passport" everyone FOC and the technology of their manufacture does not allow in essence to create two identical coding (decoding) converters. At rotation FOCвокруг of an axes of a matrix will derivate a finite sequence of matrixes of transient states of the system «the initial information - FOC». As a source of the information generating after conversion, the regular contrast strokes or lattices are used, concerning which the entry end face FOC is spun. Let's enter the angular parameter of turn $0 \le \varphi \le 2\pi$ of the kernel systems of coordinates. Then an one-parameter family of conversions

$$(K)_\varphi : (A,F)_\varphi \to (B,F')_\varphi \qquad (\overline{K})_\varphi : (B,F')_\varphi \to (A,F')_\varphi$$

Will derivate set of matrixes of transient states on the parameter j.

Resume:

1. FOC enable to generate non-determined sequences of pseudorandom numbers conjugate each other.
2. All FOC have own matrix invariants direct and converse of conversions giving possibility of generation of a gamma of keys for asymmetric systems of encoding-decoding.