© Faure E., Shvidkiy V., Shcherba A. Method of forming reproducible and unpredictable sequence of permutations // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 253-258.

МЕТОД ФОРМИРОВАНИЯ ВОСПРОИЗВОДИМОЙ НЕПРЕДСКАЗУЕМОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ПЕРЕСТАНОВОК

Эмиль Фауре, Валерий Швыдкий, Анатолий Щерба

Черкасский государственный технологический университет, Украина

ФАУРЕ Эмиль Витальевич, к.т.н.

Год и место рождения: 1983 год, г. Черкассы, Украина.
Образование: Черкасский государственный технологический университет, 2005 год.
Должность: доцент кафедры информационной безопасности и компьютерной инженерии.
Научные интересы: исследование моделей, методов и средств формирования псевдослучайных последовательностей чисел; исследование и разработка методов и средств криптографического преобразования информации; исследование кодовых и некодовых методов повышения достоверности передаваемых данных.
Публикации: более 40 научных публикаций, учебно-методические работы.
E-mail: faureemil@gmail.com

ШВЫДКИЙ Валерий Васильевич, к.т.н.

Год и место рождения: 1940 год, г. Москва, Россия.
Образование: Одесский электротехнический институт связи, 1964 год.
Должность: доцент кафедры информационной безопасности и компьютерной инженерии.
Научные интересы: исследование путей построения единых процедур кодо- и криптозащиты; синтез случайных последовательностей; исследование путей повышения пропускных способностей каналов передачи данных; сети передачи данных спецназначения.
Публикации: более 60 научных публикаций, учебно-методические работы.
E-mail: vvshv@uch.net

ЩЕРБА Анатолий Иванович, к.ф.-м.н.

Год и место рождения: 1960 год, Полтавская обл., Украина.
Образование: Харьковский государственный университет (ныне Харьковский национальный университет им. Каразина), 1982 год.
Должность: заведующий кафедрой прикладной математики.
Научные интересы: исследование свойств выпуклых тел в геометрии Минковского; исследование компонентов возрастания дельта-субгармонических функций при помощи характеристической функции Бернстейна; исследование возрастания мезоморфных и субгармонических функций; синтез случайных последовательностей.
Публикации: более 50 научных и учебно-методических работ.
E-mail: shcherba_anatoly@mail.ru

Аннотация. *В работе предлагается метод построения воспроизводимой и непредсказуемой последовательности перестановок, основанный на использовании для представления синдрома формируемой перестановки позиционной системы счисления с факториальным основанием. Для формирования синдрома следующей перестановки последовательности используется дополнительный генератор (псевдо) случайных десятичных чисел. Разработаны правила вычисления суммы факториального и десятичного чисел. Разработаны реализации предложенного метода формирования последовательности перестановок: с фиксированным нулем, со случайным нулем или с модифицированным случайным нулем. Показана возможность работы с открытым и скрытым порядком преобразования факториальной записи числа в перестановку, открытым и скрытым порядком следования перестановок в режиме реального времени.*

Ключевые слова: *перестановка, генератор перестановок, факториальная система счисления, случайное число, воспроизводимость, непредсказуемость.*

Введение

Интенсивная компьютеризация всех видов производственной, управленческой и информационной деятельности приводит к широкому применению методов моделирования производственных процессов и процессов управления сложными системами и объектами. Большую роль в создании и испытании математических и имитационных моделей устройств и процессов играют случайные последовательности чисел, в том числе, при решении задач сортировки массивов, поиска оптимальных путей обхода вершин графа, составления расписаний. Решение этих задач сводится к автоматизации процесса формирования последовательности перестановок. В силу этого обстоятельства к этой проблеме уже давно приковано внимание ученых. Наиболее известны и популярны в среде практикующих программистов труды Д. Кнута [1], Э. Рейнгольда, Ю. Нивергельта, Н. Део [2]. В частности, в этих работах изложен подход к построению перестановок, основанный на использовании позиционной системы счисления с факториальным основанием (в дальнейшем – факториальной системы). Этот подход предусматривает представление каждой из $M!$ перестановок (где M – размерность перестановки) точкой отрезка $[0, M!-1]$ числовой оси, по существу, определяющей ее порядковый номер. Таким образом, в соответствии с этим подходом порядковый номер перестановки в дискретный момент времени n, может быть представлен в виде:

$$B(n)=\sum_{i=0}^{M-1} b_i(n)\cdot w_i\,, \qquad (1)$$

где $b_i(n)$ – слово (символ), размещенное на i-той позиции;

$i\in[0, M-1]$;

w_i – вес слова, размещенного на i-той позиции.

Каждое слово $b_i(n)$ должно удовлетворять условию:

$$0\le b_i(n)\le i\,, \qquad (2)$$

а его вес – условию:

$$w_i = i!\,. \qquad (3)$$

Выражение (1) определяет размещение слов перестановки «от младшего разряда к старшему» (младший разряд слева, старший – справа).

Учитывая свойство коммутативности слагаемых суммы (1), в данной работе будет использован порядок размещения слов «от старшего к младшему». В этом случае выражение (1) примет вид:

$$B(n)=\sum_{i=0}^{M-1} b_{M-1-i}(n)\cdot w_{M-1-i}\,. \qquad (4)$$

Отметим, что выражение (4) описывает модель лототрона – вращающейся (в двух-трех плоскостях) полости с M шарами внутри, пронумерованными числами 0,1,2…(M-1).

Формирование перестановки производится последовательным извлечением шаров, причем выбор первого символа производится произвольным выбором одного из M возможных шаров (это есть старший разряд суммы (4)), выбор второго символа производится произвольным выбором одного из (M-1) возможных шаров и т.д. Выбор предпоследнего символа производится произвольным выбором одного из двух оставшихся шаров, а последний символ определяется единственным образом – последним оставшимся шаром (это есть младший разряд суммы (4)). Описанная модель процесса формирования перестановок позволяет пронумеровать все возможные перестановки при многократном повторении процесса их синтеза и служит основой (моделью) для построения генератора перестановок.

Для формирования последовательности перестановок в лексикографическом порядке предварительно по номеру предыдущей перестановки (в «n» момент времени) вычисляется номер генерируемой перестановки (в «n+1» момент времени) как

$$B(n+1)=B(n)+1\,,$$

а затем и сама перестановка.

Такой подход определяет двухэтапную процедуру преобразования порядкового номера перестановки в перестановку:

– на первом этапе создается некий образ (синдром) перестановки;

– на втором этапе синдром трансформируется в перестановку.

Синдромом перестановки $S_F(n)$ будем называть факториальную запись числа $B(n)$, а именно последовательность факториальных коэффициентов $b_i(n)$ при представлении числа $B(n)$ в факториальной системе счисления:

$$S_F(n)=b_{M-1}(n), b_{M-2}(n),..., b_1(n), b_0(n)\,. \qquad (5)$$

Замечание. В записи синдрома $S_F(n)$ используются запятые между числами $b_i(n)$, поскольку они в позиционной десятичной записи могут состоять из нескольких цифр (символов).

Последовательность $S_F(n)$ названа синдромом по той причине, что она является отпечатком (следом, отображением) перестановки $P(n)=p_{M-1}(n), p_{M-2}(n),.., p_1(n), p_0(n)$. Это значит, что по номеру $B(n)$ можно однозначно вычислить $P(n)$, а по $P(n)$ можно однозначно вычислить $B(n)$.

Генератор для формирования последовательности перестановок предложен в работе [3] и содержит:

– генератор синдрома – факториальный счетчик, на вход которого подается +1 для вычисления номера каждой следующей перестановки;

– преобразователь «синдром - перестановка» $S(n)\to P(n)$.

Известные и изложенные в работах [2, 4, 5] алгоритмы формирования перестановок отличаются правилами выполнения преобразований $S(n)\to P(n)$.

В соответствии с этими работами, наиболее развиты методы формирования перестановок, основанные на добавлении +1 к числу $B(n)$, что обеспечивает перечисление перестановок в лексикографическом порядке. При этом формирование каждой последующей перестановки основывается на вычислении $B(n)=B(n-1)+1$ с последующими преобразованиями вида $B(n)\to S(n)\to P(n)$.

Выделение нерешенных задач

Принцип лексикографического перечисления перестановок приводит к тому, что перестановки в последовательности являются предсказуемыми. Это означает, что по любой перестановке можно вычислить все последующие перестановки. Как следствие, такие генераторы не обладают криптографической стойкостью и не могут быть использованы в ряде практических приложений, в частности, в системах розыгрыша лотерей, жеребьевки спортивных состязаний, тасовки карт в электронных играх, в системах криптографической защиты информации.

Кроме того, отметим, что известные алгоритмы более или менее приемлемы для перестановок небольшой размерности, а с ростом размерности перестановки резко растет размерность задачи и, как следствие, затраты времени на ее решение, что делает невозможным использование таких алгоритмов в режиме реального времени.

Перечисленные обстоятельства стимулируют процесс создания новых методов формирования последовательностей перестановок, которые экономичны по времени, порождают случайный порядок перечисления перестановок и обладают свойствами воспроизводимости и непредсказуемости. Под свойством воспроизводимости подразумевается возможность многократного разнесенного в пространстве и (или) времени воспроизведения последовательности перестановок.

Постановка задачи

Задачей исследования является разработка метода формирования воспроизводимой непредсказуемой последовательности перестановок на основе использования факториальной системы счисления. Порождаемая последовательность перестановок должна удовлетворять требованиям:

– отсутствие корреляции между символами внутри перестановки и между смежными перестановками;

– преобразование $B(n)\to S_F(n)\to P(n)$ должно быть односторонним [6]: прямое преобразование должно быть легко выполнимым, обратное преобразование $P(n)\to S_F(n)\to B(n)$ без знания ключа должно быть невыполнимым за приемлемое время и с использованием ограниченных вычислительных ресурсов, а при использовании неправильного ключа давать ложный результат;

– последовательность перестановок должна быть невоспроизводимой без знания ключа взаимной связи смежных перестановок;

– каждая из $M!$ возможных перестановок должна встречаться в последовательности перестановок с вероятностью $1/M!$.

Решение задачи

Прежде всего:

– откажемся от выполнения операций над числом $B(n)$ и перейдем к операциям над синдромом $S_F(n)$;

– откажемся от выполнения операций вида $B(n)=B(n-1)+1$ (соответственно, и от вычисления $S_F(n)=S_F(n-1)+1$) и перейдем к операции вида

$$S_F(n)=S_F(n-1)\oplus t_{10}(n), \qquad (6)$$

где $t_{10}(n)$ – случайное число, представленное в десятичной системе счисления и обозначающее смещение порядкового номера формируемой перестановки относительно порядкового номера предшествующей перестановки на отрезке $[0,M!-1]$ числовой оси; символ $\oplus$ обозначает сложение чисел разных систем счисления – факториальной ($S_F(n-1)$) и десятичной ($t_{10}(n)$).

Случайную величину $t_{10}(n)$ формирует встроенный генератор (псевдо) случайных чисел.

Заметим, что одним из серьезных препятствий, мешающих практическому применению факториальной системы для вычисления перестановок, является необходимость обработки чисел, разрядность которых превышает несколько сот десятичных разрядов (например, при $M\ge 100$). Это обстоятельство стимулирует поиск путей, исключающих необходимость операций над числами столь большой размерности. Переход к операции над синдромом сводит выполнение процедуры вычисления перестановок к операциям над числами $0\le b_i(n)\le i$, верхнее значение которых не превышает M.

Переход к вычислению $S_F(n)=S_F(n-1)\oplus t_{10}(n)$ при случайном $t_{10}(n)$ исключает лексикографический порядок перечисления перестановок и приводит к случайному порядку их следования. В полученной последовательности перестановок степень их корреляции определяется статистическими свойствами последовательности символов $t(n)$.

Определение процедуры преобразования $S_F(n)=S_F(n-1)\oplus t_{10}(n)$.

Для реализации процедуры вычисления $S_F(n)$ по значениям $S_F(n-1)$ и $t_{10}(n)$ созданы правила вычисления:

– каждого из чисел $b_i(n)$ по заданным $b_i(n-1)$ и $t_{10}(n)$,

– символов переноса из младшего разряда в старший: $\pi_i(n)$.

Правила имеют вид:

$$b_i(n)=\left|b_i(n-1)+\pi_{i-1}(n)\right|_{i+1}, \qquad (7)$$

где $|a|_b$ – вычет (остаток) числа *a* по модулю *b*;

$$\pi_i(n) = \left[\frac{b_i(n-1) + \pi_{i-1}(n)}{i+1} \right], \quad (8)$$

где $[a]$ – целая часть числа *a*,

$$i = \overline{1, M-1},$$
$$\pi_0(n) = t(n).$$

Если дробь $\frac{a}{b}$ представить в виде $\frac{a}{b} = \mathrm{E}\left(\frac{a}{b}\right) + \varepsilon\left(\frac{a}{b}\right)$, где $\mathrm{E}\left(\frac{a}{b}\right) = \left[\frac{a}{b}\right]$ – целая часть дроби $\frac{a}{b}$, а $\varepsilon\left(\frac{a}{b}\right) = \frac{|a|_b}{b}$ – дробная часть дроби $\frac{a}{b}$, то выражения (7) и (8) примут вид:

$$b_i(n) = \varepsilon\left(\frac{b_i(n-1) + \pi_{i-1}(n)}{i+1} \right) \cdot (i+1), \quad (9)$$

$$\pi_i(n) = \mathrm{E}\left(\frac{b_i(n-1) + \pi_{i-1}(n)}{i+1} \right). \quad (10)$$

Особенностью приведенных правил является то, что операции вычисления чисел по формулам (9) и (10) выполняются в десятичной системе счисления.

Обратим внимание на то, что все числа, входящие в выражения (7)-(10), не превышают значения, равного *M*, поэтому операции над синдромом даже для перестановок большой размерности не вызывают сложностей, связанных с обработкой этих слов. В свою очередь, затраты времени на вычисление синдрома $S_F(n)$ определяются (*M*-1)-кратным выполнением операций по (7)-(10) и линейно зависят от размерности перестановки.

Следует отметить, что выражение (6) может быть модифицировано следующим образом:

$$S_F(n) = f\left(S_F(n-1)\right) + t_{10}(n), \quad (11)$$

где $f\left(S(n-1)\right)$ – некоторая функция от значения синдрома в предыдущий «*n*-1» момент времени.

В соответствии с этим, процедура модификации синдрома перестановки допускает возможность использования следующих подходов:

– формирование синдрома перестановки со случайным смещением относительно фиксированной условной нулевой точки (формирование перестановки с фиксированным нулем): $S_F(n) = S_F(0) \oplus t_{10}(n)$;

– формирование синдрома перестановки со случайным смещением относительно предшествующей условной нулевой точки (формирование перестановки со случайным нулем): $S_F(n) = S_F(n-1) \oplus t_{10}(n)$;

– формирование синдрома перестановки с модификацией случайной нулевой точки (формирование перестановки с модифицированным случайным нулем): $S_F(n) = f\left(S_F(n-1)\right) + t_{10}(n)$.

Формирование перестановки с фиксированным нулем предусматривает вычисление всех перестановок, смещенных на случайное значение $t_{10}(n)$ относительно условно выбранной нулевой точки $S_F(0)$, при этом синдром $S_F(0)$ загружается в момент пуска генератора и не меняется до завершения его работы. Такую методику формирования последовательности перестановок будем обозначать таким образом: $\left(S_F(n) = S_F(0) \oplus t_{10}(n)\right) \to P(n)$.

Особенностью этого режима синтеза последовательности перестановок заключается в том, что степень корреляции между перестановками определяется статистическими свойствами последовательности символов $t_{10}(n)$. В частности, если последовательность символов $t_{10}(n)$ является стохастической и равномерно распределенной на отрезке $[0, M!-1]$, то степень корреляции между перестановками будет равна (близка) к нулю. Если, кроме того, $t_{10}(n)$ является непредсказуемой (ключ ее образования держится в секрете), то последовательность перестановок становится непредсказуемой и криптографически стойкой.

Формирование перестановки со случайным нулем предусматривает вычисление каждой следующей перестановки, номер которой смещен на случайное $t_{10}(n)$ относительно номера предшествующей перестановки. Такую методику формирования последовательности перестановок будем обозначать таким образом: $\left(S_F(n) = S_F(n-1) \oplus t_{10}(n)\right) \to P(n)$.

Особенность такого режима синтеза последовательности перестановок заключается в том, что соседние перестановки коррелированы, что особенно проявляется при $t_{10}(n) \ll M!$. Однако если величина $t_{10}(n)$ является непредсказуемой и равномерно распределенной на отрезке $[0, M!-1]$, то последовательность перестановок также становится непредсказуемой.

Формирование перестановки с модифицированным случайным нулем предусматривает вычисление каждой следующей перестановки, синдром которой смещен на случайное значение $t_{10}(n)$ относительно подвергаемого модификации синдрома предшествующей перестановки. Модификация синдрома выполняется в соответствии с некоторым ключом преобразования, который может держаться в секрете. Ключ может распространяться на группу перестановок или подвергаться модификации от перестановки к перестановке по усмотрению пользователя. Такую методику формирования последовательности перестановок будем обозначать как

$$\left(S_F(n) = f\left(S_F(n-1)\right) \oplus t_{10}(n)\right) \to P(n).$$

Особенностью этого режима синтеза последовательности перестановок заключается в том, что по сравнению с режимом формирования перестановок со случайным нулем корреляция между соседними перестановками снижается и повышается их непредсказуемость.

Преобразование синдрома в перестановку $S_F(n) \to P(n)$.

Определим порядок преобразования синдрома в перестановку для режимов открытого и скрытного преобразования.

Открытое преобразование синдрома в перестановку описывает обратимую функцию $P(n) = G(S_F(n))$, для которой легко выполняется как прямое $\left(P(n) = G(S_F(n))\right)$, так и обратное $\left(S_F(n) = G^{-1}(P(n))\right)$ преобразования.

Скрытное преобразование синдрома в перестановку описывает обратимую функцию $P(n) = G(S_F(n))$, для которой при известном ключе легко выполняется как прямое $\left(P(n) = G(S_F(n))\right)$, так и обратное $\left(S_F(n) = G^{-1}(P(n))\right)$ преобразования, в то время как обратное преобразование $S_F(n) = G^{-1}(P(n))$ при неизвестном ключе является невыполнимым (или, как минимум, трудновыполнимым) за приемлемое время и с использованием ограниченных вычислительных ресурсов.

Целью скрытного преобразования является скрытие правил, определяющих взаимосвязь символов при преобразовании $S_F(n) \to P(n)$.

Совместное применение операций вида $S_F(n) = f(S_F(n-1)) \oplus t_{10}(n)$ (при случайном, скрываемом $t_{10}(n)$) и скрытное преобразование $S_F(n) \to P(n)$ обеспечивают скрытие взаимной связи между перестановками (соответственно, разрушает корреляционную связь между перестановками) и скрытие взаимной связи между $P(n)$ и $S_F(n)$ при преобразовании вида $P(n) \to S_F(n)$, что, в целом, повышает стойкость последовательности перестановок.

При преобразовании синдрома в перестановку входной объект преобразования – синдром $S_F(n)$, конечный продукт преобразования – перестановка $P(n)$.

Для пояснения процесса преобразования будем использовать (в качестве модели) лототрон с шарами, описываемый выражением (4). Вместо лототрона с шарами будем использовать:

– оперативное запоминающее устройство (ОЗУ);

– управляющее устройство (УУ).

Открытое преобразование

Используем ОЗУ, в которое по адресам 0, 1, 2, …, (*M*-2), (*M*-1) запишем последовательность из *M* слов в натуральном порядке – 0, 1, 2, …, (*M*-2), (*M*-1). Получим таблицу:

Таблица 1

Адрес и содержимое последовательности

Адрес	0	1	2	…	*M*-2	*M*-1
Содержимое	0	1	2	…	*M*-2	*M*-1

Пусть имеется синдром

$S_F(n) = b_{M-1}(n), b_{M-2}(n), ..., b_1(n), b_0(n)$.

На *k*-ом шаге формирования перестановки (при вычислении *k*-ого символа перестановки) выполняются следующие действия:

1. Выбирается *k*-ое слово сигнатуры со стороны старших разрядов – b_{M-k};

2. Из ОЗУ считывается слово по адресу b_{M-k}. Это слово является *k*-ым символом формируемой перестановки, т.е $p_k = R(b_{M-k})$ ($R(i)$ – содержимое ячейки ОЗУ по *i*-му адресу);

3. Извлеченное слово удаляется из ОЗУ, а все остальные слова переписываются в соответствии со следующим правилом:

$R_i \leftarrow R_i$ *для* $0 \le i \le b_{M-k} - 1$;

$R_i \leftarrow R_{i+1}$ *для* $b_{M-k} \le i \le M - k - 1$.

Указанная процедура выполняется для всех значений *k* от 1 до *M*–1.

Скрытное преобразование

Скрытное преобразование отличается от открытого тем, что при скрытном преобразовании в ОЗУ по адресам 0, 1, 2, …, (*M*-2), (*M*-1), заносится не натуральная последовательность чисел 0, 1, 2, …, (*M*-2), (*M*-1), а некая их перестановка. Эта перестановки является ключом преобразования и держится в секрете. Ключ может распространяться на группу перестановок или подвергаться модификации от перестановки к перестановке по усмотрению пользователя.

Преобразование синдрома в перестановку, использующее в качестве ключа перестановку слов натуральной последовательности чисел, эквивалентно двум последовательно выполняемым процедурам: $S(n) \to P(n)$ и последующей процедуре перестановки символов $P(n)$ по некоторой, держащейся в секрете, таблице перестановок.

Кроме того, при скрытном преобразовании и использовании процедуры вида:

$$\left(S_F(n) = f(S_F(n-1)) \oplus t_{10}(n)\right) \to P(n),$$

ключ модификации синдрома при преобразовании $f(S_F(n-1))$ также может храниться в секрете и составлять часть общего ключа преобразования. В этом случае выполнение обратного преобразования $P(n) \to S_F(n)$ на неизвестном ключе не позволяет идентифицировать $S_F(n)$.

Ключом модификации синдрома может являться перестановка длины *M*, в соответствии с которой выполняется преобразование полученной на предыдущем шаге перестановки с дальнейшим ее преобразованием в синдром. В таком случае режим формирования перестановки с модифицированным случайным нулем может быть обозначен как $\left(S(n) = f(P(n-1)) + t(n)\right) \to P(n)$.

Выводы

Выполненное исследование позволяет сформулировать следующие выводы:

– разработан метод формирования последовательности перестановок, основанный на использовании для представления синдрома формируемой перестановки позиционной системы счисления с факториальным основанием, который за счет введения дополнительного генератора случайных чисел, значения с выхода которого суммируются с синдромом предыдущей перестановки, а результат данного преобразования определяет синдром следующей перестановки, позволяет формировать воспроизводимую непредсказуемую последовательность перестановок, обладающую криптографической стойкостью;

– разработаны реализации предложенного метода в зависимости от вида процедуры вычисления синдрома следующей перестановки: формирование перестановки с фиксированным нулем $\left(S_F(n) = S_F(0) \oplus t_{10}(n)\right) \to P(n)$, формирование перестановки со случайным нулем $\left(S_F(n) = S_F(n-1) \oplus t_{10}(n)\right) \to P(n)$, формирование перестановки с модифицированным случайным нулем $\left(S_F(n) = f\left(S_F(n-1)\right) \oplus t_{10}(n)\right) \to P(n)$;

– разработаны правила вычисления суммы факториального и десятичного числа, используемые для формирования синдрома следующей перестановки в последовательности;

– разработаны два режима работы процесса формирования последовательности перестановок (открытый и скрытый), отличающиеся тем, что параметры формирования следующего синдрома перестановки, а также параметры преобразования синдрома в перестановку могут быть открытыми или составлять хранящийся в секрете ключ преобразования.

Литература

[1] Кнут Д.Э. Искусство программирования. В 7 т. — Т.4. — Вып. 2. Генерация всех кортежей и перестановок. / Дональд Эрвин Кнут, Станфордский университет; пер. с англ. Ю.Г. Гордиенко. — М. : ООО «И.Д. Вильямс», 2008. — 160 с.

[2] Рейнгольд Э. Комбинаторные алгоритмы. Теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део; пер. с англ. Е.П. Липатова; под ред. В.Б. Алексеева. — М.: Мир, 1980. — 476 с.

[3] Пат. 59628 Україна, МПК (2011.01) G11B 20/10 (2006.01), G06F 17/00. Пристрій для перебору перестановок / Борисенко О.А, Горячев О.Є.; заявник та патентовласник Сумський державний університет. — №u201012855; заявл. 29.10.2010; опубл. 25.05.2011, Бюл.№ 10. — 5 с.

[4] Борисенко О.А. Електронна система генерації перестановок на базі факторіальних чисел / О.А. Борисенко, І.А. Кулик, О.Є. Горячев // Вісник СумДУ. Технічні науки. — 2007. — №1. — С. 183-188.

[5] Горячев А.Е. Метод перебора перестановок на основе факториальных чисел / А.Е. Горячев // Вісник СумДУ. Технічні науки. — 2010. — №3. — С. 171-177.

[6] Diffie W. New directions in cryptography/ W. Diffie, M. Hellman // IEEE Information Theory Society. — New York: Institute of Electrical and Electronics Engineers. — 1976. — Vol. 22. — P. 644-654.

УДК 004.421.5 (045)

Фауре Е.В., Швидкий В.В., Щерба А.І. Метод формування відтворюваної непередбачуваної послідовності перестановок

Анотація. *У роботі пропонується метод побудови відтворюваної та непередбачуваною послідовності перестановок, що базується на використанні позиційної системи числення з факторіальною основою для представлення синдрому перестановки. Для формування синдрому наступної перестановки послідовності використовується додатковий генератор (псевдо) випадкових десяткових чисел. Розроблено правила обчислення суми факторіального і десяткового чисел. Розроблено реалізації запропонованого методу формування послідовності перестановок: з фіксованим нулем, з випадковим нулем або з модифікованим випадковим нулем. Показано можливість роботи з відкритим і прихованим порядком перетворення факторіального запису числа в перестановку, відкритим і прихованим порядком слідування перестановок у режимі реального часу.*

Ключові слова: *перестановка, генератор перестановок, факторіальна система числення, випадкове число, відтворюваність, непередбачуваність.*

Faure E., Shvidkiy V., Shcherba A. Method of forming reproducible and unpredictable sequence of permutations

Abstract. *In this paper, we propose the method for constructing a repeatable and unpredictable sequence of permutations based on the use of positional notation with factorial base to represent syndrome of formed permutation. For the formation of syndrome of the next permutation in the sequence an additional generator of (pseudo) random decimal numbers is used. The evaluation rules of summing of decimal and factorial numbers are developed. The next implementations of the method of forming sequence of permutations are developed: with a fixed zero, with a random zero or with a modified random zero. The possibility of working with the overt and covert order of transformation of the factorial record of number into permutation and the overt and covert permutations order in real time is shown.*

Key words: *permutation, permutation generator, factorial number system, random number, reproducibility, unpredictability.*

Отримано *30 вересня 2014 року*, затверджено редколегією *16 жовтня 2014 року*