# СТОХАСТИЧЕСКАЯ КРИПТОГРАФИЯ. ДИХОТОМИЧЕСКИЕ ПОСЛЕДОВАТЕЛЬНОСТИ И ИХ СВОЙСТВА

**Кулаков Игорь Анатольевич**
http://random-art.ru/

Закладываются концептуальные основы стохастических технологий нового поколения и представляемой ими стохастической криптографии, минималисткой и легковесной по исполнению и существу. Производится обобщение и распространение свойств, присущих натуральному ряду на так называемые дихотомические последовательности. Дается анализ дихотомических последовательностей и их свойств, в обычной арифметике, в предшествующей ей неполной арифметике и предарифметике. Приведены примеры уравнений их генерации. Отмечается многомерный, параметрический, существенно выраженный нелинейный характер способов генерации таких последовательностей. Указывается на возможность достижения функциональной неразрешимости по существу, при сравнительно малых аппаратных затратах и крайне высокой эффективности схем реализаций.

Первая статья аналогичного содержания была написана по материалам доклада на 3-ей Центрально-европейской конференции по криптологии в Братиславе, **TATRACRYPT′**03 [1]. С этой статьи началась публикация результатов, полученных на протяжении многолетних исследований и экспериментальных разработок в области нелинейной динамики [2], стохастических систем, криптографии и технологий обеспечении безопасности [3]. С тех пор прошло много времени, многое, особенно с открытием предарифметики [4], датируемым сентябрем 2006 года, а позже (2007-2010 г.) и ее разновидностей [5], стало более понятным и ясным, и многое изменилось. Поэтому возникла необходимость обновления и публикации новых, полученных за этот период научно-технических результатов.

**Обозначения элементарных двоичных операций**:

$\&, |, \oplus, \overline{\oplus}, \bar{}$ – операции **AND**, **OR**, **XOR**, **XNOR** и инверсии **NOT**, соответственно, над $n$-разрядами ($n \geq 1$) двоичными величинами;

$\prec_m, \succ_m$ – смещение на $m$ разрядов ($m \geq 0$) в сторону старших и младших бит;

$z \bmod 2^n$ – остаток от деления на $2^n$ или тоже, что ограничение изменения разрядов переменной $z$ & $(2^n - 1)$ числом $n$ значащих бит.

Для начала обратимся к двоичному представлению первых чисел натурального ряда, начиная с нуля:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **00** | 0000 | **04** | 0100 | **08** | 1000 | **12** | 1100 |
| **01** | 0001 | **05** | 0101 | **09** | 1001 | **13** | 1101 |
| **02** | 0010 | **06** | 0110 | **10** | 1010 | **14** | 1110 |
| **03** | 0011 | **07** | 0111 | **11** | 1011 | **15** | 1111 |

Рис.1

Из образованной таким образом из двоичной последовательности $C = \{c_i: i = \overline{1,m}\}$, составленной из элементов $c_i \in C$, разрядностью $m = 4$ бит, видно, что период повторения $T_k$ каждого очередного $k$-го бита, равен $T_k = 2^k$ $(k = \overline{1,n})$, для произвольного $n$. Кроме этого, для каждого $k$-го бита, элементы $i$ и $(i+T_k/2)$, принадлежащие соседним полупериодам этой последовательности $C$, комплементарны

$$c_{ki} = \bar{c}_{k(i+Tk/2)}, \qquad (1)$$

т.е. связаны между собой операцией комплементации $\bar{}$ **NOT**.

Двоичная последовательность $C$, представленная на Рис.1, задается ***единичным счетчиком инкрементного типа*** – $c_i = c_{i-1} + 1 \bmod 2^4$, а обратная, рекуррентная к ней последова-

тельность $C^*$, задается ***единичным счетчиком <u>декрементного типа</u>*** – $c^*_i = c^*_{i-1} - 1 \ mod \ 2^4$, соответственно.

К этому, аналогичной структурой и свойствами наделены все двоичные последовательности, формируемые на основе ***линейного (смешанного) конгруэнтного метода*** [6,7] с $n$-битовой двоичной переменной $x$, задаваемого уравнением:

$$x_i = a \cdot x_{i-1} + b \ \ mod \ 2^n, \qquad (2)$$

при $a \equiv 1(mod\ 4)$ и нечетном $b$. Кардинальное число $card\ X$ множества всех таких аналогичных различных двоичных последовательностей с максимальным периодом $T_n = 2^n$, при различных значениях коэффициентов $\{a,b\}$ и начальных условий $x_0$, равно $2^{3(n-1)}$.

Заметим, ***линейный конгруэнтный метод*** (2) ***<u>носит неполный характер</u>***, и согласно результатам, приведенным в [5,8], допускает простое развитие:

$$x'_i = a' \cdot (x'_{i-1} \oplus h) + b' \ \ mod \ 2^n, \qquad (3)$$

при $a' \equiv 3(mod\ 4)$, нечетном $h$ и четном $b'$. Кардинальное число $card\ X'$ множества всех таких различных двоичных последовательностей, равно $2^{4(n-1)}$, а при $h = 1$, $card\ X' = 2^{3(n-1)}$.

В отличие от предшествующего ему линейного уравнения (2), ***данное уравнение*** (3), что само по себе уже показательно, ***<u>носит явно выраженный нелинейный характер</u>***. В силу этого, в отличие линейного конгруэнтного метода (2), криптографический анализ таких последовательностей (3), в особенности сильно усеченных, на 64 бит и более младших значащих бит, затруднен [9].

Более того, коэффициенты $\{a,b,h\}$, входящие в состав уравнений (2) и (3), согласно исследованиям и полученным результатам [2,3,8] при выполнении соответствующих условий синхронизации, могут быть переменными, со скрытым, неизвестным для стороннего наблюдателя, но непременно обладающим дихотомическими свойствами, законом изменения составляющих их бит. В этих случаях криптографический анализ таких последовательностей, не только затруднен, но и носит непреодолимый, соизмеримый с полным перебором, функционально сложный и неопределенный характер.

Принимая во внимание сказанное, данные результаты допускают следующее естественное обобщение и дальнейшее продолжение.

Двоичная последовательность $D = \{d_i : i = \overline{1, T_n}\}$, составленная из $n$-битовых элементов $d_{ik}$ $(k = \overline{1, n})$, называется ***дихотомической - D*** или ***Dh-последовательностью***, если частотные изменения значений каждого его $k$-го двоичного разряда носит регулярный характер, при котором любая из подпоследовательностей, образованная из элементов исходной последовательности путем исключения $D \ mod \ T_k$ их $n-k \in [0,n-1]$ старших разрядов, имеет период повторения $T_k = 2^k$ и в пределах его не содержит одинаковых элементов, т.е. ***обладает свойствами <u>апериодичной последовательности</u>***.

Другими словами, распределение значений последовательности $D$, составленной ровно из $T_n$ элементов $d_j \in D$, обладает иерархической структурой типа двоичного дерева, состоящей из $n$ уровней $k \in [1,n]$ и $m_k = T_n / T_k$ взаимно непересекающихся на этих $k$ уровнях, идентичных *дихотомических классов* $D_k \equiv D\ (mod\ T_k)$, при этом любая одноразрядная двоичная пара $\{d_{ki}, d_{ki}+T_k/2\}$ ее $i$ и $i+T_k/2$ элементов $(i = \overline{1, T_n - T_k/2})$, разделенных полупериодом $T_k/2$, комплементарна, т. е. $\bar{d}_{ki} = d_{ki}+T_k/2$.

Двоичные величины, обладающие указанными свойствами, именуются *дихотомическими величинами*, а возникающий при этом порядок - *дихотомическим порядком* [2,3]. По индукции, следуя с первого уровня до последнего, легко показать, что нарушение условий комплементарности, влечет нарушение условий апериодичности.

Для дальнейшего изложения, введем понятие $\alpha$*-среза* двоичной последовательности $B = \{b_i\}$, состоящей из конечного числа $n$-битовых элементов $b_i$, представляющего собой дво-

ичную подпоследовательность $B_\alpha$, где $\alpha \in [1,n]$, составленную из множества $\{b_{i\alpha}\}$ бит $b_{i\alpha} \in \{0,1\}$, взятых по номеру $\alpha$ из каждого $b_i$ элемента, исходной для нее последовательности $B$.

По определению, $D$-последовательности и их срезы $D_\alpha$, обладают следующими свойствами:

1. Подпоследовательности $D_k = D \bmod T_k$ $(k = \overline{1,n})$, $n$-разрядной двоичной $Dh$-последовательности $D$, полученные путем усечения ее элементов $d_i \in D$ со стороны старших значащих бит, есть последовательности максимальной длины, иначе, как принято в литературе, *М-последовательности*, с периодом повторения $T_k = 2^k$.
2. $D_k$-последовательности бесповторны (апериодичны) в пределах периода $T_k$ и порождают дихотомический порядок.
3. Период $T_k$ среза $k$, экспоненциально нарастает $T_k = 2^k$, с ростом его номера $k$.
4. Все пары битов $\{b_{ki}, b_{k\,(i+\,Tk/2)}\}$ $k$-среза, разделенные полупериодом $T_k/2$, комплементарны между собой – $b_{ki} = \overline{b}_{k\,(i+\,Tk/2)}$.
5. По определению, число нулевых и единичных битов в любом из периодов среза, равны.

Следуя дальше, уравнение формирования $D$-последовательностей, в некотором роде и в функциональном пределе подчиняющихся линейным и полиномиальным законам [8], с кардинальным числом, равным произведению периодов срезов:

$$card\, P = 2^n \cdot 2^{n-1} \cdot 2^{n-2} \cdot \ldots 2^1 \cdot 1 = 2^{n(n+1)/2}, \qquad (4)$$

можно задать следующим рекуррентным выражением:

$$X_i = a_o + \sum_{k=1}^{n} a_k x_{k\,(i-1)} 2^{k-1} \bmod 2^n \qquad (x_{k\,(i-1)} \in 0,1), \qquad (5)$$

где $a_o\ a_k$ – нечетные постоянные коэффициенты, приращение и множители из интервалов $[1,2^n - 1]$ и $[1,2^{n-k+1} - 1]$, соответственно, и условии $a_1 \equiv 1 (\bmod 4)$. Кардинальное число $card\, X$ множества всех таких различных $D$-последовательностей равно $2^{n(n+1)/2}$ и совпадает с кардинальным числом (4) , полученным выше исходя из произведения периодов срезов.

Аналогично линейному конгруэнтному методу (2) и его расширению (3), указанный метод (5) допускает развитие [1,3]:

$$X'_i = a'_o + \sum_{k=1}^{n} a'_k (x'_{k(i-1)} \oplus h_k) 2^{k-1} \bmod 2^n \qquad (x'_{k\,(i-1)} \in 0,1), \qquad (6)$$

при четном $a'_o$, нечетных коэффициентах $a'_k \in [1,2^{n-k+1} - 1]$ и нечетном модификаторе $h = \{h_k \in 0,1: k = \overline{1,n}\}$, а также при соблюдении условия, что $a'_1 \equiv 3 (\bmod 4)$. Кардинальное число $card\, X'$ множества всех таких различных $D$-последовательностей, как и в предшествующем случае (5), при $h = 1$, также равно $2^{n(n+1)/2}$.

В такой постановке, в отличие от предшествующего ему линейного уравнения (5), ***данное уравнение*** (6), по отношению к уравнению (3), в силу использования смешанных операций $\{+,\oplus\}$, ***носит явно выраженный нелинейный характер***. По всему, криптографический анализ таких последовательностей (6), в особенности сильно усеченных, если судить по материалам исследований [9], весьма проблематичен.

Аналогично, как и в упомянутых ранее уравнениях (2) и (3), при выполнении соответствующих условий синхронизации коэффициент $h$ может быть переменным, с неизвестным для стороннего наблюдателя, дихотомическим законом изменения составляющих его бит. В этих случаях криптографический анализ таких последовательностей, в силу формального усечения $h$, носит непреодолимый, не иначе как полным перебором, функционально сложный и неопределенный характер.

Перебирая поразрядно полупериоды всех дихотомических классов, порождаемых обычным арифметическим счетчиком $D_i = D_{i-1} + E \bmod 2^n$ по всем ограниченным полупериодом начальным условиям и возможным приращениям $E$, можно определить кардинальное

число $card\,D$ множества всевозможных различных *Dh*-последовательностей:

$$card\,D = 2^{2^{1-1}-1}\cdot 2^{2^{2-1}-1}\cdot 2^{2^{3-1}-1} \ldots \cdot 2^{2^{n-1}-1}\cdot 2^{n-1}\cdot 2^{1} = 2^{2^{n}-1}. \qquad (7)$$

В итоге, принимая во внимание указанные положения, уравнение формирования всевозможных, различных *Dh*-последовательностей, может быть задано следующим рекуррентным выражением:

$$X_i = (a_0 \oplus b_0) + \sum_{k=1}^{n} A_k(x_k, x_{k-1}, \ldots, x_1)_{i-1}\, 2^{k-1} \bmod 2^{n} \quad (x_{k\,(i-1)} \in 0,1), \qquad (8)$$

при нечетном *n*-разрядном приращении $a_0$ и коэффициенте $a_1$, синхропараметре $b_0$, равным 0 или 1, и суперпозиции [10] одночленов (мономов):

$$A_k(x_k, x_{k-1}, \ldots, x_1) = x_k + \sum_{(i_1,\ldots,i_{k-1})} a_{i_1,\ldots,i_{k-1}} x_1^{i_1} \cdot \ldots\, x_{k-1}^{i_{k-1}} \qquad (k > 1,\ i_{k-1} \in 0,1) \qquad (9)$$

и мономе $A_1 = (a_1 + 2\cdot b_0)\cdot(x_1 \oplus b_0)$, $a_1 \equiv 1 (mod\ 4)$, где $\sum_{(i_1,\ldots,i_{k-1})} a_{i_1,\ldots,i_{k-1}} x_1^{i_1} \cdot \ldots\, x_{k-1}^{i_{k-1}}$ означает суммирование по всем различным сочетаниям одноразрядных двоичных переменных $\{x_k\} \in X$, числом $2^{2^{k-1}}$.

Суммирование по всем мономам, начальным условиям и приращениям дает кардинальное число $card\,X = 2^{2^{n}-1}$ множества всех таких различных *Dh*-последовательностей.

Совпадение кардинальных чисел $card\,X = card\,D = 2^{2^{n}-1}$, по Кантору, означает, что ***любая из возможных Dh-последовательностей <u>может быть единственным образом</u> выражена через коэффициенты уравнения*** (9). С тем же успехом, как и в предшествующих двух случаях, в уравнение (8) можно ввести постоянный или переменный коэффициент $h$.

Как видим, число всевозможных *Dh*-последовательностей, даже при небольших $n$, необъемно огромно и охватывает гармоничные, упорядоченные процессы и существенно неупорядоченные, хаотичные процессы. В последнем случае закон распределения изменений в старших разрядах быстро стремится к идеальному равномерному.

В такой постановке, в отличие от предшествующего уравнения (6), ***данное уравнение*** (8), способно приобретать ***<u>существенно выраженный нелинейный характер</u>***. В силу этого, криптографический анализ формируемых на его основе последовательностей, в особенности усеченных, как показывают проведенные исследования [1-3], вполне может носить непреодолимый, сравнимый с полным перебором, функционально сложный и неопределенный характер.

***Математические доказательства*** построения последовательностей максимального периода в соответствии с представленными выше уравнениями – ***<u>отсутствуют</u>***, за исключением элементарного случая (2), довольно глубоко исследованного и подробно изложенного [6]. Для того чтобы указанные доказательства стали возможными, необходимо осознать новые и вскрыть еще не известные нам математические структуры и представляемые ими основы и глубины развития теории чисел.

***<u>Несмотря на отсутствие доказательств</u> – все утверждения подтверждены результатами натурного моделирования и расчетами***. Сомневающиеся могут все это проверить или довериться результатам исследований [1-5,8]. По всему – это один из тех редких случаев, когда практика далеко опережает теорию.

Следуя здравому смыслу, исходящего из прикладного характера проводимых работ, необходимо отметить, что ***<u>описание</u>*** и тем более формирование *Dh*-последовательностей, представляемых уравнением (9), ***является непомерно громоздким, вычислительно сложным и слабо предсказуемым*** по принятым криптографическим меркам и статистическим показателям, что делает данный подход непригодным для практики.

В академическом, нежели чем в практическом плане, малое и при этом не столь эффективное исключение, в силу использования относительно высоко затратной операции умножения, составляют ряды, свойственные конгруэнтному методу [8,9], его линейному представлению (2) и его нелинейному расширению (3).

В целом, разрешить указанные выше проблемы и довести формирование *Dh*-последовательностей до математической прозрачности, должного прикладного и эффективного практического результата, оказалось возможным благодаря работе [2] и последовавшим из нее открытию Предарифметики [4].

Между тем, здесь будет уместно напомнить, что в отличие от нерегулярных частотных свойств, присущих разрядам (срезам) *n*-битовых случайных двоичных последовательностей с идеальным равномерным законом распределения, свойственным истинно случайным процессам, ***распределение частот*** срезов *Dh*-последовательностей, ***носит регулярный характер***. Такой, частотно регулярный характер изменения срезов обусловлен регулярным изменением периода, равным $2^k$ ($k = \overline{1,n}$), в зависимости от номера среза – *k*.

В силу этого младшим битам *Dh*-последовательностей, присуща существенно выраженная корреляция. Корреляция убывает от младших битов *Dh*-последовательности, к старшим. По мере убывания корреляции, старшие биты, способны приобретать существенно выраженный недетерминированный, по существу функционально непредсказуемый, неразрешимый характер.

Как показано в ранее проведенных [1-3,11-14] и последних работах [15], при достижении необходимых статистических и функциональных показателей старших значащих бит *Dh*-последовательностей, указанные недостатки, связанные с частотно регулярным характером изменения их элементов, могут быть элементарно устранены, посредством введения простых стохастических преобразований ее элементов [16-18].

В этих условиях, получение надежных в статистическом и функциональном, а с ними и в криптографическом отношении случайных последовательностей может быть осуществлено путем преобразований элементов исходных для них *Dh*-последовательностей, направленных на ***сокрытие дихотомических и выравнивание частотных свойств значащих битов***. При этом преобразования упомянутых элементов представляются простыми и эффективными (биективными, сюръективными) функциями усложнения, построенным на основе элементарных принципов рассеяния и перемешивания битов и ее элементов [3,11,16-18].

Следует отметить, что присущие данному алгебраическому направлению недостатки, связанные с регулярными частотными изменениями и введением функций усложнения, могут быть нивелированы или устранены, за счет введения в обратных связей в представленные уравнения. Правда, при этом утрачиваются бесповторные (апериодичные) свойства, но это уже отдельная тема [3,12,16,18].

Открытие **Предарифметики** (Pre-Arithmetic, Prearithmetic), как видится, знаменует начало развития новой алгебраической базы, по функциональным, системным и техническим показателям значительно превосходящей поля Галуа. Позже, в период с 2007 по 2010 год, были открыты и другие ее разновидности [5].

Как показывают результаты многолетних исследований, введение предарифметики и следующих из нее разновидностей, позволит обогатить теорию чисел, физику и математику, а с ними осуществить качественный скачек в развитии теории динамических и стохастических систем дискретного времени, нелинейной динамики и теории Хаоса.

***Предарифметики и представляемые ими алгебраическая база послужили основой для создания стохастических технологий***, направленных, в первую очередь, для построения высококачественных генераторов случайных чисел, двоичных нелинейных функций, односторонних и однонаправленных функций, хэш-функций, поточных (потоковых) и блочных шифров. Иначе говоря, по прикладным результатам и содержанию – ***симметричной*** (***стохастической***) ***криптографии*** в целом, как показывают предварительные результаты [18], характеризующейся подавляющим превосходством по всем показателям перед существующими аналогами, по своей сути, не в ущерб криптографической стойкости и достигаемым техническим показателям ***являющейся одновременно и минималисткой и легковесной***.

Многолетние исследования в области динамических систем [2], Предарифметики [5], представляемая ими алгебраическая база и стохастические технологии, в итоге, послужили

созданию, представляемого на тематическом сайте [15], отраженного заявками на изобретение – рандомизационного способа.

**Рандомизационный способ** (Random Method) делится на регулярный и нерегулярный. В регулярном способе, распространение влияния младших битов цифровых блоков на старшие, носит строго однонаправленный, ламинарный характер. В нерегулярном способе разряды цифровых блоков, ко всему, охвачены обратными связями.

**Регулярный рандомизационный способ** [17] предназначен для формирования упомянутых *Dh*-последовательностей, на основе, так называемых, ***дихотомических генераторов*** [11]. В свою очередь, дихотомические генераторы могут быть взаимосвязаны между собой и способны образовывать сети и композиции любой структурной и функциональной сложности [2,3], и служат основой для построения высококачественных генераторов случайных чисел, поточных (потоковых) шифров и стохастических систем дискретного времени различного назначения.

**Нерегулярный рандомизационный способ** [18] более широк, наследует основные (структурные и функциональные) свойства регулярного способа [2,3,17], закладывает основы для построения блочных шифров и по своим характеристикам и статистическим показателям вплотную примыкает к идеальному Хаосу и истинно случайным процессам [12].

Хотя данное направление еще молодо, но уже хорошо развито и доведено до схемотехнических решений [15], необходимых для изготовления высокорентабельных промышленных образцов, по статистическим, функциональным и техническим показателям, недостижимо далеко опережающим все известные на сегодня аналоги [19].

В итоге, обобщая имеющиеся материалы, выделим наиболее важные свойства присущие дихотомическим последовательностям и представляемым их уравнениям, а именно:

1. Частотные свойства, выражающиеся в экспоненциальном росте периода повторения от бита к биту.
2. Комплементарные свойства, связывающие полупериоды отрицанием НЕ.
3. Бесповторные свойства, характеризующиеся отсутствием повторений в пределах периода.
4. Лавинные свойства, обусловленные ускоренным распространением влияния младших битов на старшие, включая нелинейное распространение влияния битов посредствам операции XOR.
5. Нелинейные свойства, вносимые конъюнкцией AND младших битов со старшими.
6. Функциональная неопределенность, обусловленная сложным, параметрическим и переменным характером изменения коэффициентов вводимых в состав представляемых уравнений генерации (8).
7. Способность образовывать, обладающие дихотомическими свойствами многомерные структурные (сетевые) композиции любой сложности [2].
8. Мультипликативное комплексирование с $m$-разрядными регистрами сдвига с линейной обратной связью (LFSR), с периодом $T = 2^n (2^m - 1)$, но в этом случае утрачиваются бесповторные свойства [17,18].

Анализ показывает, что параметризация и многомерность позволяет достичь функциональной неразрешимости уравнений генерации по существу, это с одной стороны. С другой на функциональную (криптографическую) силу дихотомических генераторов указывает лавинная, экспоненциальная скорость распространения влияния и существенно нелинейная катенация младших битов со старшими.

При этом, посредством выбора структурных композиций и их параметризации [2,8], эта сила может быть существенно увеличена и регулируема в широких пределах.

**Ключевые слова**: динамическая, стохастическая, система, предарифметика, алгебра, нелинейная динамика, линейный, полиномиальный, конгруэнтный, метод, дихотомический,

порядок, дихотомическая, последовательность, дихотомический, генератор, симметричная, минималистская, легковесная, стохастическая, криптография, генерация, случайных, псевдослучайных, чисел, односторонние, однонаправленные, функции, поточные, потоковые, блочные, шифры, рандомизационный, регулярный, нерегулярный, стохастический, способ.

**Литература**[*]


1. Кулаков И. А., Дихотомические последовательности и их свойства. Материалы доклада на 3-ей Центрально-европейской конференции в Братиславе, TATRACRYPT 2003, Словакия, 28 июня 2003.
2. Кулаков И. А. Способ придания реальному объекту рандомизационных свойств и рандомизационная система. Международная заявка PCT/RU03/00141 от 7 апреля 2003. Заявка на Евразийский патент №200500946 от 11 июля 2005.
3. Кулаков И. А.. Стохастические системы и криптография. Материалы конференции РусКрипто 2006, Москва, февраль 2006
4. Кулаков И. А. Предарифметика. Рукопись статьи, май, 2011.
5. Кулаков И. А. Гипотеза о природе Арифметики. Рукопись статьи, июль, 2011.
6. Кнут Дональд Э. Искусство программирования. Третье издание, Том 2, М.: Издательский дом “Вильямс”, 2002.
7. Шнайер Брюс. Прикладная криптография. Изд. ТРИУМФ, Москва, 2002.
8. Кулаков И. А.. Полиномиальный конгруэнтный метод с переменными коэффициентами и его нелинейные расширения. Рукопись статьи, 2012.
9. Brickell et al. A Surkey of Recent Results. Proc. of the IEEE, Vol. 76, no. 5, May 1988.
10. Глухов М. М., Елизаров В. П., Нечаев А. А. АЛГЕБРА. М.: Гелиос АРВ, 2003.
11. Кулаков И. А.. Дихотомические генераторы и их свойства. Материалы 6-й Международной конференции по информационной безопасности и криптологии, ICISC 2003, Сеул, 27 ноября 2003.
12. Кулаков И. А.. Рандомизационные генераторы. Материалы 11-й Международной конференции по быстрым программным средствам шифрования, FSE 2004, Нью-Дели, 5 февраля 2004.
13. Кулаков И. А., Куксов С. Н., Дятленко А. В., Филиппов Н. В. Система контроля сертификационных меток промышленных товаров НИР, Московский комитет по науке и технологиям, Москва, апрель 2005.
14. Иванов А. Г., Иванов М. А., Дударев Д. А., Кулаков И. А. Анализ алгоритма односторонней аутентификации. Экспертные заключения. Московский комитет по науке и технологиям, Москва, июль 2006.
15. Кулаков И. А. Тематический сайт, русская и англоязычная версии. http://t.random-art.ru/recommendation/, февраль-март 2012.
16. Кулаков И. А. Линейные конгруэнтные и рандомизационные генераторы. Рукопись статьи, 2012.
17. Кулаков И. А. Способ формирования регулярных последовательностей. Российская и Международная заявки на изобретение, август 2011 года.
18. Кулаков И. А. Способ формирования нерегулярных последовательностей. Российская и Международная заявки на изобретение, август 2011 года.
19. Кулаков И. А. Оценка статистических, функциональных и технических показателей Рандомизационного способа. Тематический сайт, 2011 года.


**МОСКВА, март 2012**

[*] Одноименные статьи автора можно найти в рубрике СТАТЬИ тематического сайта RANDOM-ART.RU.