КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ ДИХОТОМИЧЕСКИХ ГЕНЕРАТОРОВ

Обозначения элементарных двоичных операций :

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

$\lhd_m, \rhd_m$ – 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;

$\overline{\&}^C$ – нелинейная управляемая двоичная операция **NAND**/**NOR** над n-разрядами двоичными величинами $\{a,b\}$, с управляющей переменной c, вида:

$$a \ \overline{\&}^C \ b = (a \,\&\, b) \ \overline{\oplus} \ (c \,\&\, (a \oplus b)). \qquad (1)$$

В данной работе ограничимся постановкой и решением задачи оценки криптографических показателей так называемых дихотомических *Dh*-генераторов, построенных на основе материалов, представляемых регулярным рандомизационным способом: http://random-art.ru/?download=PPC%20Patent.pdf (раздел 6).

Согласно с ним, представляемые для анализа и оптимальные в реализации *Dh*-генераторы задаются следующими рекурсивными уравнениями:

$$P_i = ((G_{i-1} \ \overline{\&}^C \ P_{i-1}) \lhd_1) \oplus H_P, \qquad G_i = G_{i-1} \oplus P_{i-1} \oplus (G_{i-1} \lhd_3) \ \bmod 2^n, \qquad (2)$$

с n-разрядными двоичными переменными – базовой G переменной, ее нелинейным дополнением P и управляющей C переменной:

$$C = (G_{i-1} \lhd_1) \,\&\, \overline{3}, \qquad (3)$$

при начальных условиях $\{P_O,G_O\}$, с произвольной, нечетной по величине n-разрядной постоянной H_P, меньшей 2^n, – двоичным модификатором H_P. Требование нечетности обусловлено условиями синхронизации уравнений (2), необходимым для получения *Dh*-последовательностей, характеризуемых максимальным периодом $T_{max} = 2^n$ и бесповторностью в пределах периода входящих в их состав элементов.

Из результатов проведенных исследований, представленный уравнениями (2) рекурсивный процесс имеет короткий переходной нелинейный участок L_m, не превышающий n ($L_m \leq n$), быстро исчезающий в результате феноменальной самосинхронизации, после которого формируемые на их основе последовательности $\{G_i\}$, причем, независимо от начальных условий $\{P_O,G_O\}$ и модификатора H_P, нечетного по определению, переходят в дихотомические, с максимальным периодом $T_{max} = 2^n$ и с неповторяющимися в пределах периода составляющими ее элементами.

Анализ также показывает, что число разнообразных *Dh*-последовательностей, формируемых на основе уравнений (2) с учетом всевозможных 2^{n-1} значений модификатора H_P, равно $2^{n+(n-1)}$, а не $2^{2 \cdot n + (n-1)}$, как можно было бы ожидать исходя из всего разнообразия $2^{2 \cdot n}$ начальных условий $\{P_O,G_O\}$. Данный факт обусловлен процессом самосинхронизации и вызываемым им последовательным переходом в стационарное состояние, завершающимся с преодолением переходного участка L_m, при этом переход в стационарное состояние ведет к строгой (инъективной) функциональной зависимости $P = Đ(G)$ нелинейного дополнения P от базовой G переменной. Обратная функция $Đ^{-1}$ носит неоднозначный (сюръективный) характер.

Число разнообразных *Dh*-последовательностей, можно значительно увеличить, до $2^{4(n-1)}$, посредством модификации входящих в состав упомянутого уравнения переменных $\{G,C\}$. А именно:

$$P_i = ((G_H \&^{C_H} P_{i-1}) \lhd_1) \oplus H_P, \quad G_i = G_H \oplus P_{i-1} \oplus (G_H \lhd_3) \ \bmod 2^n, \qquad (4)$$

$$G_H = H_G \oplus G_{i-1}, \quad C_H = H_C \oplus C = H_C \oplus ((G_{i-1} \lhd_1) \,\&\, \overline{3}), \qquad (5)$$

при произвольных, четных по величине модификаторах $\{H_G,H_C\}$, меньших 2^n.

Ниже, в Таблице, представлен алгоритм и программная реализация *Dh*-генераторов на языке С, с выходом, ориентированным на формирование истинно и псевдослучайных случайных последовательностей, шифрирующих гамм и аутентификацию.

Таблица

***Dh*-ГЕНЕРАТОРЫ. АЛГОРИТМ И ПРОГРАММА РЕАЛИЗАЦИИ**
Исходные данные: n – длина платформы генерации, бит. Начальные условия – $\{p_o, g_o\}$. Константы: $Cm = 2^n - 1 = (Cs - 1) \mid Cs$ при $Cs = 1<< (n-1)$; C0 = 0; C1 = 1; C_1 = Cm ^ 1; C_3 = Cm ^ 3; Hp = 0, Hp = 1 или Hp = Rp, где Rp - случайное число. Исследуемые двоичные переменные: G – базовая переменная; P – нелинейное дополнение; R – выходная переменная. **Управляющая переменная**: c = (G<<1) & C_3.

Программа:
G = g; **P** = p; **R** = (G ^ P) & Cm;
p = (p<<1) | C1; g ^= p;
p = (G & p) ^ (c & g) ^ Hp;
g ^= G<<3;
 	
Тестовые примеры генерации, для двух крайних случаев, при использовании управляемой операции **AND**/**OR** – Hp = C0 и операции **NAND**/N**OR** – Hp = Cm, при n = 20 и нулевых начальных условиях $p_o = g_o = 0$, приведены на эпюрах фиг.1 и фиг.2, соответственно.

Примечание. Для получения *Dh*-последовательностей, отображаемых базовой переменной – *G*, требуется *n* холостых итераций, позволяющих гарантированно исключить наблюдаемые на эпюрах переходные участки. Формируемые таким образом *Dh*-последовательности будут иметь максимальный период $T_{max} = 2^n$, с неповторяющимися в пределах периода элементами. Как показывает статистический анализ на основе пакета DIEHARD, старшие значащие разряды *G* базовой *R* выходной переменной представленных *Dh*-генераторов, начиная с 26-го, независимо от начальных условий и модификатора Hp, имеют статистические свойства, мало отличающиеся от свойств, присущих истинно случайным величинам.

Элементарный анализ *Dh*-генераторов (2), показывает, что такие генераторы не являются криптографически стойкими и просто вскрываются, при движении от младших разрядов к старшим. Более того, в силу дихотомических свойств, присущих таким генераторам, изменения разрядов которых, начиная с первого самого младшего, носят регулярный характер, с периодом 2^k ($k = \overline{1, \boldsymbol{n}}$), что делает младшие биты фактически непригодными для прямых практических приложений. Кроме этого, в связи со строго однонаправленным характером распространения влияния младших битов на старшие, имеет место явно выраженный, убывающий от младших и старших битов неравнозначный по сложности вклад младших и старших битов начальных условий $\{P_O, G_O\}$ и модификаторов $\{H_P, H_G, H_C\}$, а равно с ними и вклад младших и старших разрядов элементов последовательности, формируемых на основе указанных *Dh*-генераторов.

Исходя из всего этого, далее ограничимся рассмотрением исключительно *Dh*-генераторов, в программном исполнении задаваемым представленным в Таблице алгоритмом, с усеченным выходом со стороны младших $k < n$ значащих бит, или просто

усеченных *Dh*-генераторов, в следующей постановке.

Постановка задачи.

1. Разработка методики и программы, позволяющих при различных значениях *n* и разумной по времени длительности счета, по известной части старших (*n*-*k*) значащих бит **R** выходной переменной, вычислить неизвестные начальные условия {po,go} и определить значение модификатора Hp нелинейного дополнения **P**, при различном числе *k* усекаемых младших бит выходной переменной **R**.

2. Разработка методики и программы выработки оценок вычислительной сложности вскрытия начальных условий {po,go} и определения выступающего в качестве параметра *Dh*-генератора модификатора Hp, измеряемых исходя из числа элементарных логических операций, типа AND и XOR.

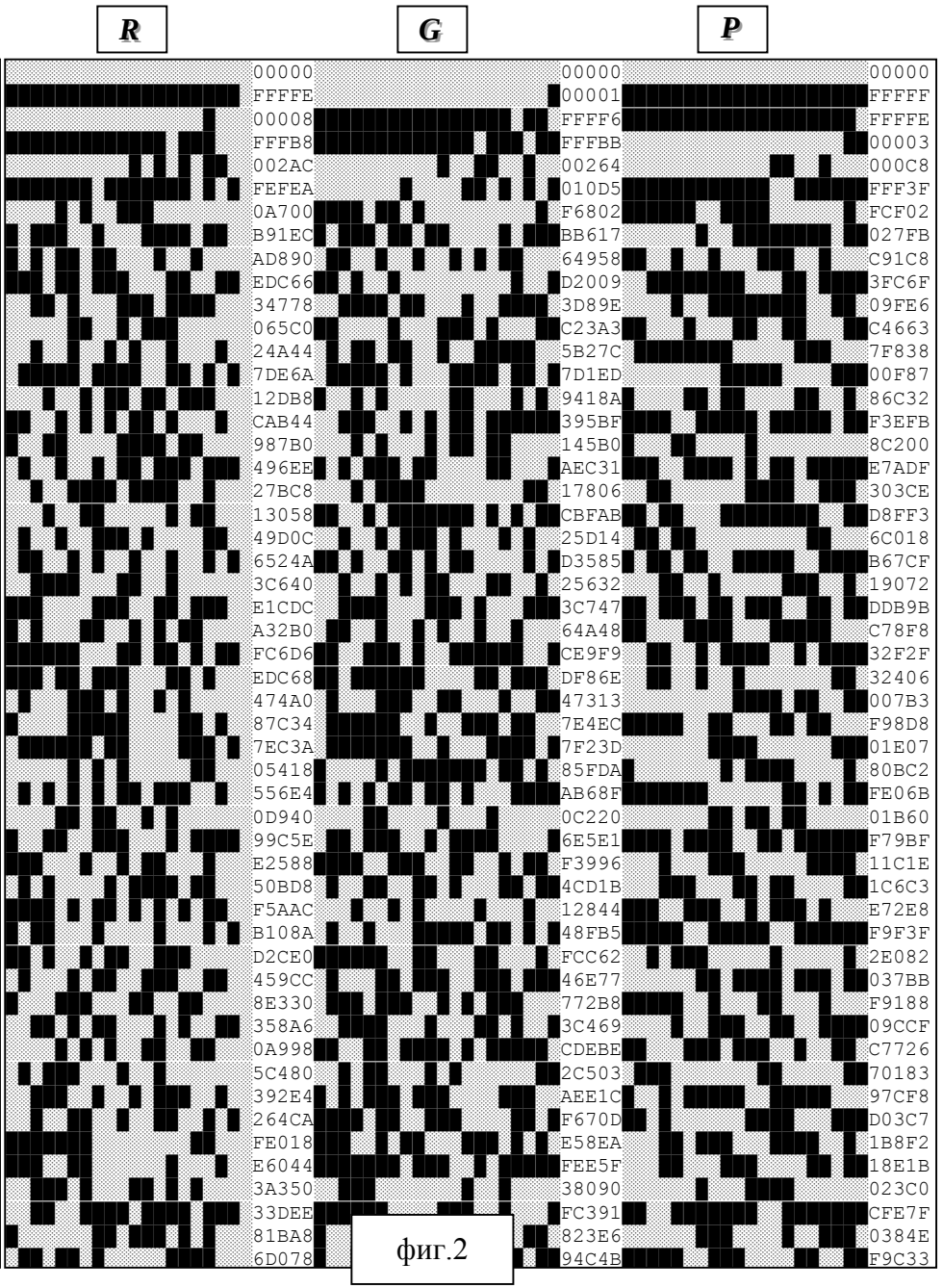
3. Разработка методики и программы выработки оценок вычислительной сложности вскрытия усеченных *n*-разрядных *Dh*-генераторов, посредством экстраполяции результатов на большие платформы генерации.

4. Распространение решений и выработка аналитических оценок вычислительной сложности вскрытия *Dh*-генераторов, переменные {g,c} которых, согласно с условиями синхронизации (66), подвергаются модификации: g ^= Hg и c ^= Hc, при четных модификаторах {Hg,Hc}.

Решение данных задач, представляемых регулярным рандомизационным способом закладывает фундаментальную базу для реализации двоичных потоковых генераторов псевдослучайных чисел, легковесных и энергоэкономичных протоколов аутентификации, рассчитанных на среды с крайним дефицитом ресурса.


R
G
P
00000 00000 00000
00001 00001 00000
00009 00008 00001
0004B 0004B 00000
00213 00212 00001
01283 01281 00002
0868D 0868C 00001
4B6E7 4B2EF 00408
10D5B 12D86 020DD
84983 8000D 0498E
89365 89378 0001D
C0AFB C0883 00278
448EB C486A 80081
60A7B E0A39 80042
25B45 E5B74 C0031
892D7 480B7 C1260
0A12B 8A1CE 800E5
DAFBB DAE75 001CE
9D0BD 0DE40 90EFD
4AD7B 431BB 09CC0
4B453 485E2 031B1
0CA73 0C991 003E2
6015D 682DC 08381
694A7 3933F 50798
602CB 505F6 3073D
D2BC3 B243D 60FFE
01655 E1A28 E0C7D
ECBEB 2D393 C1878
CCC4B C7FFA 0B3B1
698BB EE749 87FF2
5CD25 922E4 CEFC1
0AD87 9EA47 947C0
7F97B 437FE 3CE85
62AFB 21505 43FFE
AFDDD AC2D0 03F0D
C6CDB CAA4B 0C690
1F933 87532 98C01
8BC83 8C4A1 07822
ED1AD E11EC 0C041
31FC7 F1E0F C01C8
1F3FB FEDE6 E1E1D
34303 CBEED FFDEE
B4D85 6B258 DFFDD
7299B 8DF23 FF6B8
8342B 1CB4A 9FF61
FB11B C6FD9 3DEC2
45305 8AC94 CFF91
DCA37 43717 9FD20
60BEB 675EE 07E05
1DB5B 52695 4FDCE
C863D 5E9A0 96F9D
BA0BB 87B9B 3DB20

фиг.1


R
G
P
00000 00000 00000
FFFFE 00001 FFFFF
00008 FFFF6 FFFFE
FFFB8 FFFBB 00003
002AC 00264 000C8
FEFEA 010D5 FFF3F
0A700 F6802 FCF02
B91EC BB617 027FB
AD890 64958 C91C8
EDC66 D2009 3FC6F
34778 3D89E 09FE6
065C0 C23A3 C4663
24A44 5B27C 7F838
7DE6A 7D1ED 00F87
12DB8 9418A 86C32
CAB44 395BF F3EFB
987B0 145B0 8C200
496EE AEC31 E7ADF
27BC8 17806 303CE
13058 CBFAB D8FF3
49D0C 25D14 6C018
6524A D3585 B67CF
3C640 25632 19072
E1CDC 3C747 DDB9B
A32B0 64A48 C78F8
FC6D6 CE9F9 32F2F
EDC68 DF86E 32406
474A0 47313 007B3
87C34 7E4EC F98D8
7EC3A 7F23D 01E07
05418 85FDA 80BC2
556E4 AB68F FE06B
0D940 0C220 01B60
99C5E 6E5E1 F79BF
E2588 F3996 11C1E
50BD8 4CD1B 1C6C3
F5AAC 12844 E72E8
B108A 48FB5 F9F3F
D2CE0 FCC62 2E082
459CC 46E77 037BB
8E330 772B8 F9188
358A6 3C469 09CCF
0A998 CDEBE C7726
5C480 2C503 70183
392E4 AEE1C 97CF8
264CA F670D D03C7
FE018 E58EA 1B8F2
E6044 FEE5F 18E1B
3A350 38090 023C0
33DEE FC391 CFE7F
81BA8 823E6 0384E
6D078 94C4B F9C33

фиг.2