А.Е. Жуков
директор ассоциации РусКрипто

Поточные шифры в начале XXI века

The State of the Art of Stream Ciphers

eSTREAM - ECRYPT Stream Cipher project (2004 - 2008)

http://www.ecrypt.eu.org

ECRYPT Stream Cipher project (2004 - 2008)

- Конкурс eSTREAM проводился при поддержке Еврокомиссии в рамках программы ECRYPT.

Этапы конкурса

- 14-15.10.2004 — SASC 2004 (Bruges) - The State of the Art of Stream Ciphers
- 01.11.2004 - 29.04.2005 — представление материалов на конкурс eSTREAM.
- 05.2005 — Начало 1-й фазы конкурса
- 2-3.02.2006 — SASC 2006 (Leuven)
- 07.2006 — Начало 2-й фазы конкурса
- 31.01-1.02.2007 — SASC 2007 (Bochum)
- 04.2007 — Начало 3-й фазы конкурса
- 04.2008 — Итоговый отчет ECRYPT Stream Cipher project: The eSTREAM Portfolio

Требования к кандидатам

- Профиль 1. Поточные шифры, ориентированные на программную реализацию. Должны поддерживать 128-битный ключ и IV длиной 64 или 128 бит.
- Профиль 2. Поточные шифры, ориентированные на аппаратную реализацию в том числе при ограниченных ресурсах памяти, ограничениях на число логических элементов или источники питания. Должны поддерживать 80-битный ключ и IV длиной 32 или 64 бита.

Алгоритмы, представленные на конкурс eSTREAM

Профиль 1

1. ABC
2. CryptMT/Fubuki
3. DICING
4. DRAGON
5. Frogbit A
6. HC-256
7. Mir-1
8. Py
9. Salsa20
10. SOSEMANUK

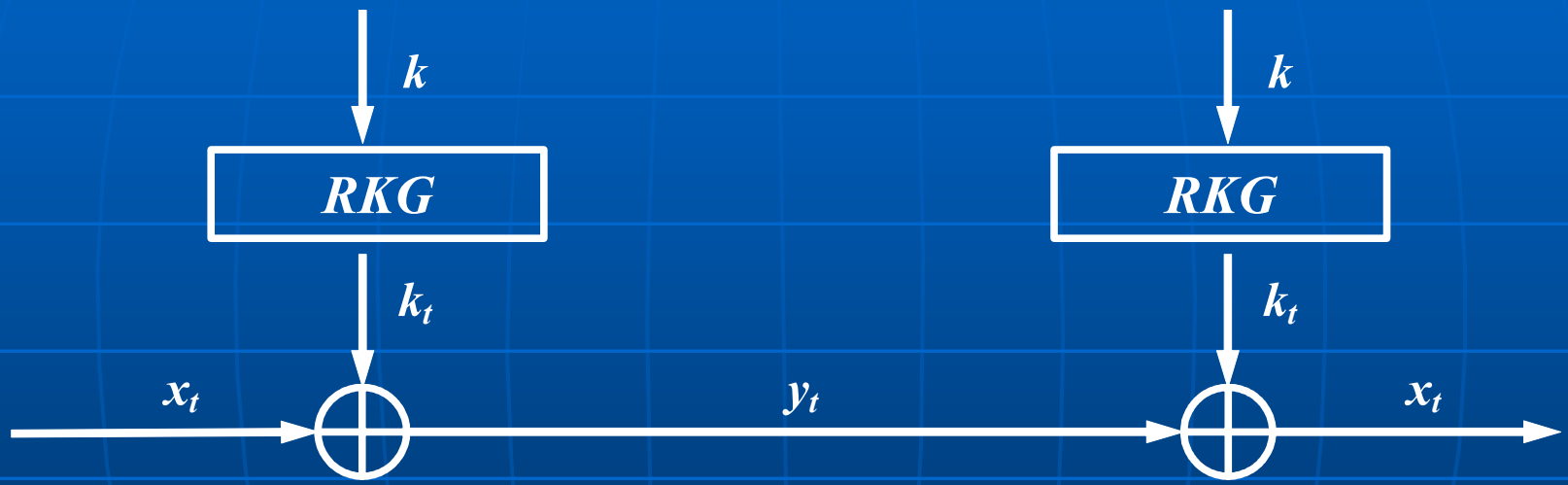
Профиль 1,2

1. F-FCSR
2. Hermes8
3. LEX
4. MAG
5. NLS A
6. Phelix A
7. Polar bear
8. POMARANCH
9. Rabbit
10. SSS A
11. TRb DK3 YAEA
12. Yamb

Профиль 2

1. Achterbahn
2. DECIM
3. EDON-80
4. Grain
5. MICKEY
6. MICKEY-128
7. MOSQUITO
8. SFINKS A
9. Trivium
10. TSC-3
11. VEST A
12. WG
13. ZK-Crypt

Аддитивный синхронный поточный шифр



По-прежнему наиболее распространенный тип поточного шифра (шифр гаммирования)

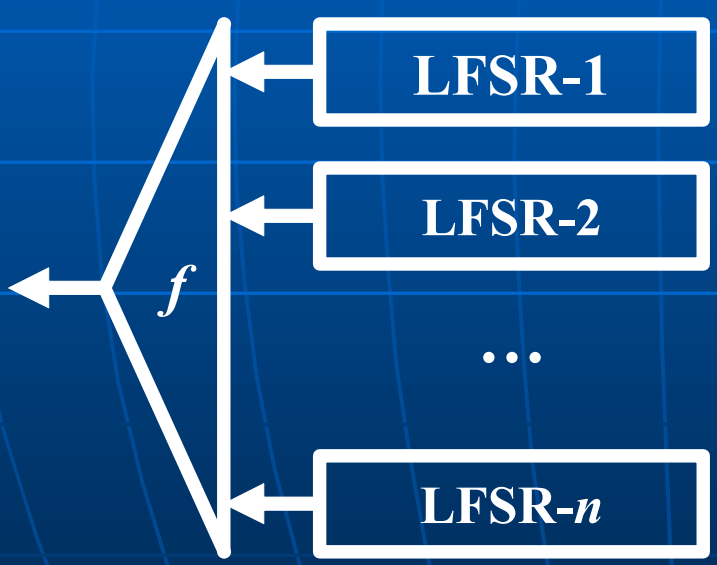
RKG – Running Key Generator

Рассматривая *RKG* как автономный автомат, Руппель выделял в конструкции типичного *RKG* *управляющую часть* (*driving part*) и *комбинационную часть* (*combining part*).

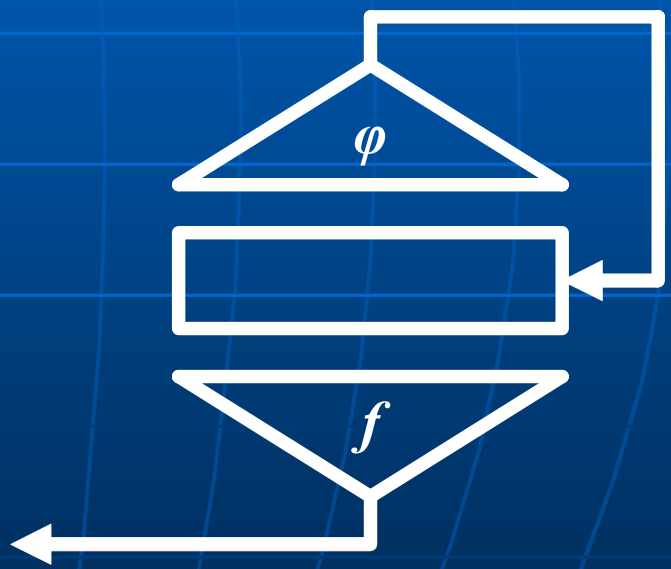
Управляющая часть задает переход из одного внутреннего состояния автономного автомата в другое и обеспечивает большой период и хорошие статистические свойства выходной последовательности.

Комбинационная часть непосредственно принимает участие в выработке знаков выходной последовательности и отвечает за ее сложность и непредсказуемость, не разрушая при этом хороших свойств, обеспечиваемых управляющей частью.

Комбинирующие и фильтрующие генераторы

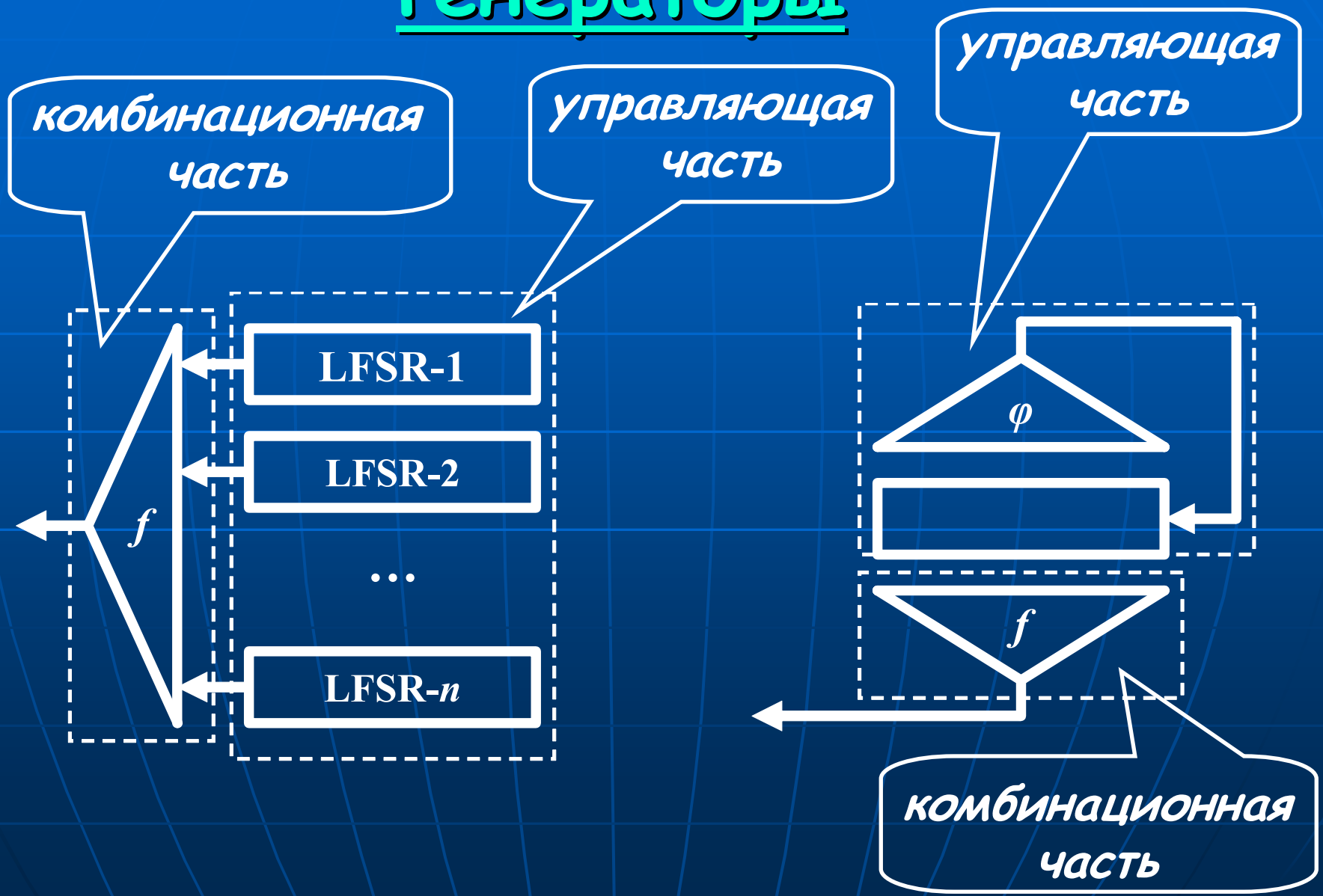


Комбинирующий генератор



Фильтрующий генератор

Комбинирующие и фильтрующие генераторы



Устройство управляющей части

- **LFSR:** ABC, Decim, Grain, MICKEY-128, Polar Bear, Sfinks, SOSEMANUK, WG, Yamb, ZK-Crypt
- **Jump Controlled LFSR:** Pomaranch
- **FCSR:** F-FCSR-H
- **NFSR:** Achterbahn, Dragon, Grain, MICKEY-128, NLS, SSS, Trivium, VEST, CryptMT-Fubuki

Устройство управляющей части

- **Динамические массивы:** HC128, Hermes8, Mir1, MAG (cellular automata), Phelix, Rabbit, Polar Bear, Py, Salsa20/12, Edon80, Mosquito, TSC-3

- **Счетчики:** NLS, Rabbit
  - **MAC/Hash:** Phelix, Salsa20/12
  - **Блочные шифры:** LEX

Устройство комбинирующей части

- **Нелинейные функции усложнения:** ABC, Decim, Grain, MICKEY-128, WG

  - **Использование отдельных узлов блочных шифров** Phelix, Salsa20/12, Hermes8
  - **или целиком блочных алгоритмов:** LEX

Устройство комбинирующей части

- **Прореживание промежуточной гаммы :** ABC, Decim, Grain, Polar Bear, MICKEY-128, Sfinks, Yamb, SOSEMANUK, WG

- **Использование конечных автоматов для улучшения промежуточной гаммы:** Pomaranch

Оригинальные разработки

- DICING:
- Edon80: pipelined architecture of 80 simple 2-bit transformers called e-transformers
- Frogbit:
- Mosquito: type of finite state machine — a conditional complementing shift register (CCSR)
- TSC-3:
- Py, Phelix - from Portfolio report

Участники 3-й фазы конкурса

По профилю 1	По профилю 2
Rabbit	Trivium
Salsa20/12	Grain v.1
SOSEMANUK	F-FCSR-H v.2
HC-128	MICKEY v.2
NLS v.2	Decim v.2
LEX v.2	Edon80
CryptMT v.3	Pomaranch v.3
Dragon	Moustique

The eSTREAM Portfolio

- Предложенное «portfolio» содержит наиболее удачные алгоритмы, из числа представленных на конкурс eSTREAM.
- В отличии от конкурса AES (или предстоящего конкурса SHA-3) здесь не определяется «абсолютный победитель».

Жюри конкурса

- S. Babbage (Vodafone, UK)
- C. De Canniere (Katholieke Univ. Leuven, Belgium)
- A. Canteaut (INRIA, France)
- C. Cid (Royal Holloway, Univ. of London, UK)
- H. Gilbert (France Telecom R&D, France)
- T. Johansson (Lund Univ., Sweden)
- C. Paar (Ruhr-University of Bochum, Germany)
- M. Parker (University of Bergen, Norway)
- B. Preneel (Katholieke Univ. Leuven, Belgium)
- V. Rijmen (Graz Univ. of Technology, Austria)
- M. Robshaw (France Telecom R&D, France)
- H. Wu (Katholieke Univ. Leuven, Belgium)

Результаты голосования

По профилю 1		По профилю 2	
Rabbit	2.80	Trivium	4.35
Salsa20/12	2.80	Grain v.1	3.50
SOSEMANUK	1.20	F-FCSR-H v.2	0.52
HC-128	0.60	MICKEY v.2	0.17
NLS v.2	-0.60	Decim v.2	-1.38
LEX v.2	-1.20	Edon80	-1.72
CryptMT v.3	-1.40	Pomaranch v.3	-2.24
Dragon	-1.60	Moustique	-2.50

Результаты голосования

По профилю 1		По профилю 2	
Rabbit	2.80	Trivium	4.35
Salsa20/12	2.80	Grain v.1	3.50
SOSEMANUK	1.20	F-FCSR-H v.2	0.52
HC-128	0.60	MICKEY v.2	0.17
NLS v.2	-0.60	Decim v.2	-1.38
LEX v.2	-1.20	Edon80	-1.72
CryptMT v.3	-1.40	Pomaranch v.3	-2.24
Dragon	-1.60	Moustique	-2.50

Алгоритмы, вошедшие в портфолио конкурса eSTREAM

Апрель 2008 г.

По профилю 1	По профилю 2
HC-128	F-FCSR-H v.2
Rabbit	Grain v.1
Salsa20/12	MICKEY v.2
SOSEMANUK	Trivium

F-FCSR-H v.2

M. Hell and T. Johansson.
Breaking the F-FCSR-H stream cipher in Real Time.
In J. Pieprzyk, editor,
Proceedings of Asiacrypt 2008

Алгоритмы, вошедшие в портфолио конкурса eSTREAM

На сентябрь 2008 г.

По профилю 1
HC-128
Rabbit
Salsa20/12
SOSEMANUK

По профилю 2
Grain v.1
MICKEY v.2
Trivium

Алгоритмы, вошедшие в портфолио конкурса eSTREAM

По профилю 1		
HC-128	Hongjun Wu	Institute for Infocomm Research, Singapore
Rabbit	M.Boesgaard, M.Vesterager, T.Christensen, E.Zenner	CRYPTICO, Denmark
Salsa20/12	Daniel J. Bernstein	The University of Illinois, USA
SOSEMANUK	C.Berbain, O.Billet, A.Canteaut, N.Courtois, H.Gilbert, L.Goubin, A.Gouget, L.Granboulan, C.Lauradoux, M.Minier,T.Pornin, H.Sibert	France Telecom, INRIA, Ecole Normale Superieure, France

Алгоритмы, вошедшие в портфолио конкурса eSTREAM

По профилю 1		
HC-128	Hongjun Wu	Singapore
Rabbit	M.Boesgaard, M.Vesterager, T.Christensen, E.Zenner	Denmark
Salsa20/12	Daniel J. Bernstein	USA
SOSEMANUK	C.Berbain, O.Billet, A.Canteaut, N.Courtois, H.Gilbert, L.Goubin, A.Gouget, L.Granboulan, C.Lauradoux, M.Minier,T.Pornin, H.Sibert	France

Алгоритмы, вошедшие в портфолио конкурса eSTREAM

По профилю 2		
Grain v.1	M.Hell, T.Johansson, W.Meier	Lund University, Sweden FH Aargau, Switzerland
MICKEY v.2	S.Babbage, M.Dodd	Vodafone Group R&D, UK
Trivium	C.de Canniere, B.Preneel	Katholieke Universiteit Leuven, Belgium

Алгоритмы, вошедшие в портфолио конкурса eSTREAM

По профилю 2		
Grain v.1	M.Hell, T.Johansson, W.Meier	Sweden Switzerland
MICKEY v.2	S.Babbage, M.Dodd	UK
Trivium	C.de Canniere, B.Preneel	Belgium

Программно-ориентированные поточные шифры

Профиль 1

Реализация алгоритмов профиля 1

- 2000MHz (one of two CPU cores) AMD Athlon 64 X2
- 533MHz (one of two CPUs) Motorola PowerPC G4 7410
- 1300MHz Intel Pentium M
- 900MHz AMD Athlon
- 440MHz (one of two CPUs) HP 9000/785 J5000
- 3000MHz Intel Pentium 4
- 1000MHz (one of two CPUs) Intel Pentium III
- 900MHz Sun UltraSPARC III
- 2800MHz (one of two CPUs) Intel Pentium 4
- 1900MHz Intel Pentium 4
- 400MHz DEC Alpha EV5.6 21164A
- 133MHz Intel Pentium

Скорость программной реализации поточных шифров профиля 1 с 256-битным ключом

Результаты приведены для Intel Pentium 4 3000MHz

Шифрование большого объема данных

Алгоритм	Скорость (тактов на байт)
HC-128	3.6
Rabbit	5.1
SOSEMANUK	5.7
Salsa20/12	8.1
AES (counter mode)	33.1

Установка ключа и шифрование 40-байтного пакета

Алгоритм	Скорость (тактов на байт)
Rabbit	33.5
Salsa20/12	44.9
AES (counter mode)	51.6
SOSEMANUK	64.2
HC-128	686.1

Rabbit

Martin Boesgaard
Mette Vesterager
Thomas Christensen
Erik Zenner

CRYPTICO A/S, Denmark

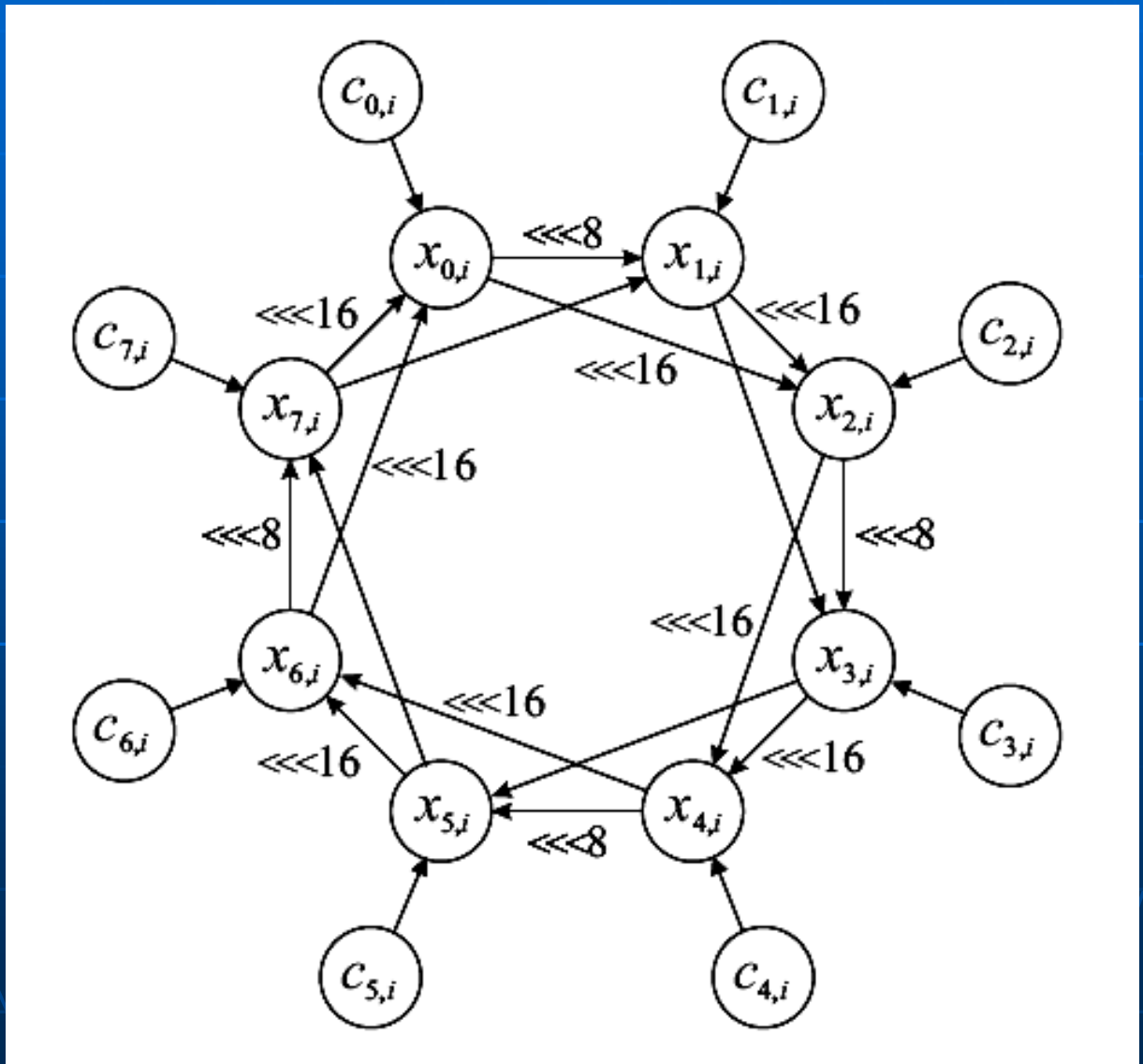
Rabbit

Работа алгоритма определяется 128-битным секретным ключом и 64-битным IV (если таковой используется).

Внутреннее состояние соответствующего автомата определяется 513 битами: восемь 32-битных регистров внутренних переменных, восемь счетчиков с 32-битными состояниями и однобитный счетчик бита переноса.

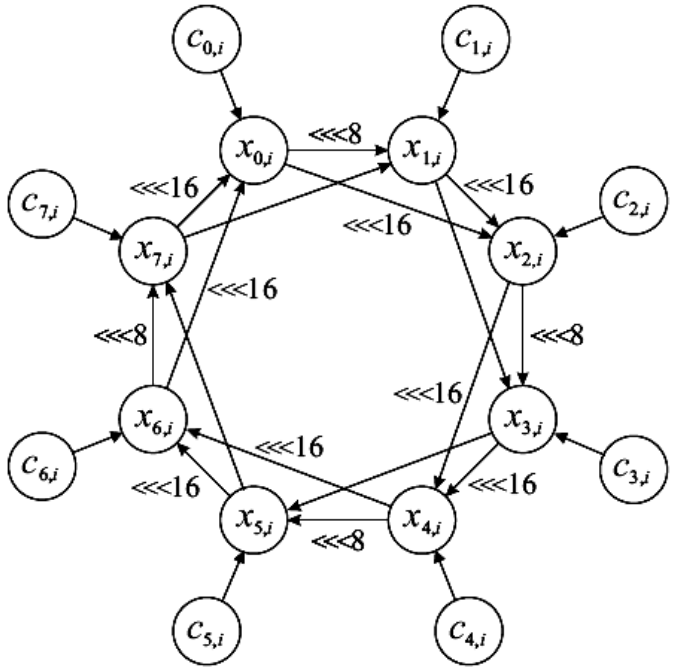
Выходом является последовательность 128-битных блоков, определяемых линейной функцией внутреннего состояния. На одном 128-битном ключе можно шифровать не более 2^{64} блоков открытого текста.

Rabbit


$c_{0,i}$
$c_{1,i}$
$x_{0,i}$
$x_{1,i}$
$\lll 8$
$\lll 16$
$c_{7,i}$
$c_{2,i}$
$x_{7,i}$
$x_{2,i}$
$\lll 16$
$\lll 16$
$\lll 16$
$\lll 8$
$\lll 8$
$\lll 16$
$x_{6,i}$
$x_{3,i}$
$c_{6,i}$
$c_{3,i}$
$\lll 16$
$\lll 16$
$\lll 16$
$x_{5,i}$
$x_{4,i}$
$\lll 8$
$c_{5,i}$
$c_{4,i}$

Rabbit

$$x_{0,i+1} = g_{0,i} + (g_{7,i} \ll 16) + (g_{6,i} \ll 16)$$
$$x_{1,i+1} = g_{1,i} + (g_{0,i} \ll 8) + g_{7,i}$$
$$x_{2,i+1} = g_{2,i} + (g_{1,i} \ll 16) + (g_{0,i} \ll 16)$$
$$x_{3,i+1} = g_{3,i} + (g_{2,i} \ll 8) + g_{1,i}$$
$$x_{4,i+1} = g_{4,i} + (g_{3,i} \ll 16) + (g_{2,i} \ll 16)$$
$$x_{5,i+1} = g_{5,i} + (g_{4,i} \ll 8) + g_{3,i}$$
$$x_{6,i+1} = g_{6,i} + (g_{5,i} \ll 16) + (g_{4,i} \ll 16)$$
$$x_{7,i+1} = g_{7,i} + (g_{6,i} \ll 8) + g_{5,i}$$



$$g_{j,i} = (x_{j,i} + c_{j,i+1})^2 + ((x_{j,i} + c_{j,i+1})^2 \gg 32) \bmod 2^{32}$$

$$c_{j,i+1} = c_{j,i} + a_j + \varphi_{j-1,i+1} \bmod 2^{32}$$

$$\varphi_{j,i+1} = \begin{cases} 1, & \text{если } c_{0,i} + a_0 + \varphi_{7,i} \geq 2^{32} \text{ и } j = 0; \\ 1, & \text{если } c_{j,i} + a_j + \varphi_{j-1,i+1} \geq 2^{32} \text{ и } j > 0; \\ 0 & \text{в остальных случаях.} \end{cases}$$

Salsa20/12

Daniel J. Bernstein

Department of Mathematics, Statistics and Computer Science

The University of Illinois at Chicago

Chicago, USA

Salsa20/12

Работа алгоритма определяется 32-байтным (256-битным) или 16-байтным (128-битным) секретным ключом.

В основе алгоритма лежит хэш-функция Salsa, имеющая 64-битный вход и выход.

Выходом является последовательность 64-битных блоков. Очередной блок является хэш-функцией от ключа, 8-байтного номера сообщения и номера очередного блока. На одном ключе можно шифровать не более 2^{70} байт открытого текста.

The eSTREAM Portfolio

- Алгоритм SNOW 2.0, представленный на конкурс NESSIE, также может быть включен в портфолио по Профилю 1 (программно-ориентированные шифры).

Апаратно-ориентированные поточные шифры

Профиль 2

Аппаратная реализация AES-128 (технология ASIC)

Архитектура	8-bit	32-bit	64-bit	128-bit
Число S-блоков	1	4	8	20
Число тактов на 1 блок	1032	54	32	11
Скорость [битов за такт]	0,12	2,37	4,00	11,64
Тактовая частота [MHz]	80	131	137	145
Скорость [Mbps]	9,9	311	548	1691

Аппаратная реализация AES-128 (технология FPGA)

Архитектура	8-bit	32-bit
Число S-блоков	1	4
FPGA	Xilinx Spartan II XC2S15-6	Xilinx Spartan II XC2S30-6
Тактовая частота [MHz]	67	60
Скорость [Mbps]	2.2	69

Скорость аппаратной реализации поточных шифров профиля 2

Аппаратная реализация поточных шифров профиля 2

Алгоритм	Площ. (μm^2)	Тактовая частота [MHz]	Скорость [битов за такт]	Скорость [Gbit/s]	Эффект. (Gbit/ s_mm^2)	Эффект. в сравнении с AES
Trivium	144	312	64	18.5	128.8	68.3
Grain v.1	120	300	16	4.4	37.4	19.8
MICKEY v2	82	308	1	0.2	3.5	1.9
AES (OFB)	280	182	3.12	0.5	1.8	1.0

Trivium

Christophe De Cannière
and
Bart Preneel

Katholieke Universiteit Leuven
Belgium

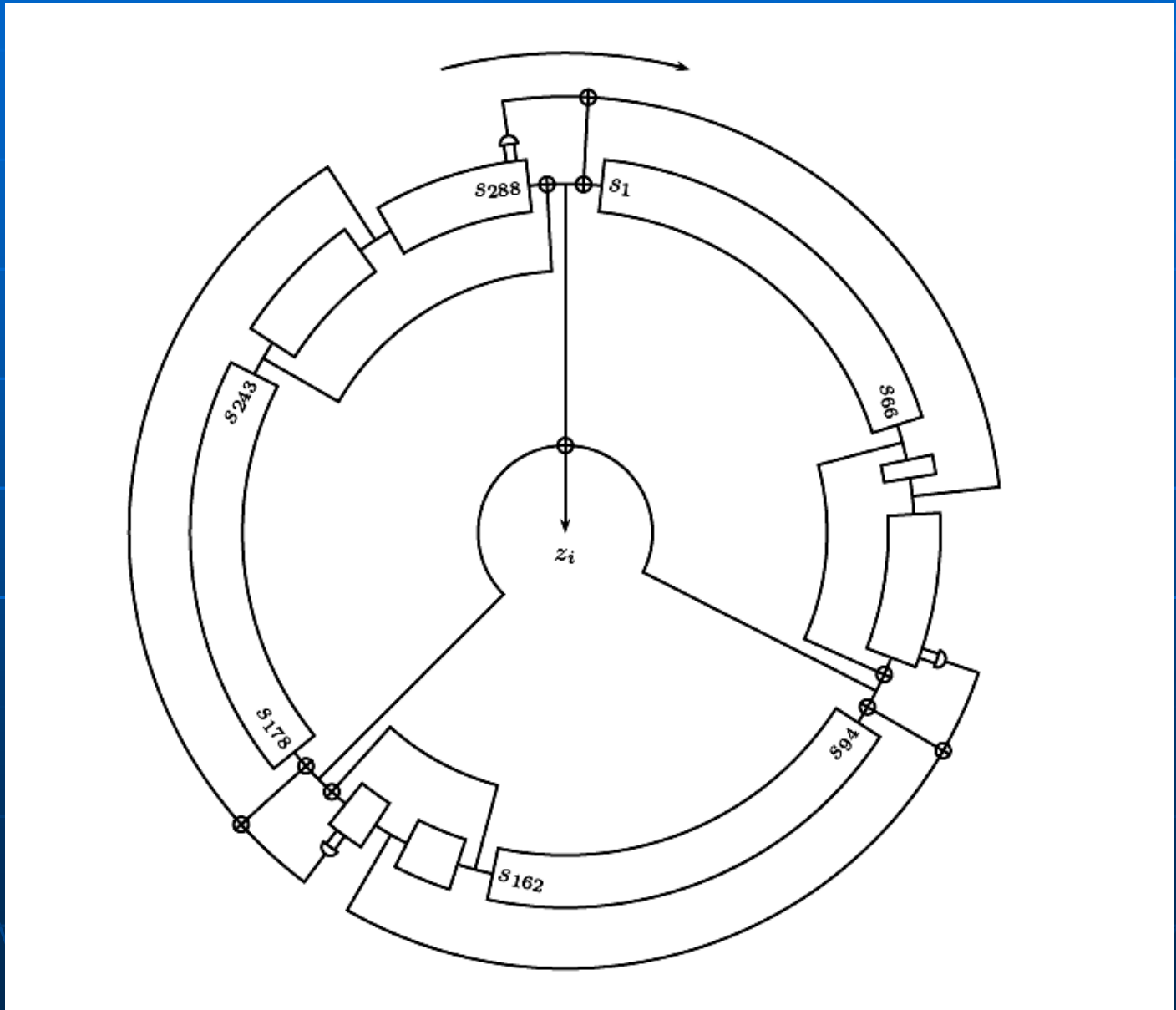
Trivium

Работа алгоритма определяется 80-битным секретным ключом и 80-битным IV.

Внутреннее состояние соответствующего автомата определяется 288 битами, объединенными в три нелинейных регистра сдвига по 93, 84 и 111 бит соответственно.

Выходом является битовая последовательность, определяемая как сумма съемов с каждого из регистров.

Trivium



Trivium

for $i = 1$ to N do

$t_1 \leftarrow s_{66} + s_{93}$

$t_2 \leftarrow s_{162} + s_{177}$

$t_3 \leftarrow s_{243} + s_{288}$

$z_i \leftarrow t_1 + t_2 + t_3$

$t_1 \leftarrow t_1 + s_{91} \cdot s_{92} + s_{171}$

$t_2 \leftarrow t_2 + s_{175} \cdot s_{176} + s_{264}$

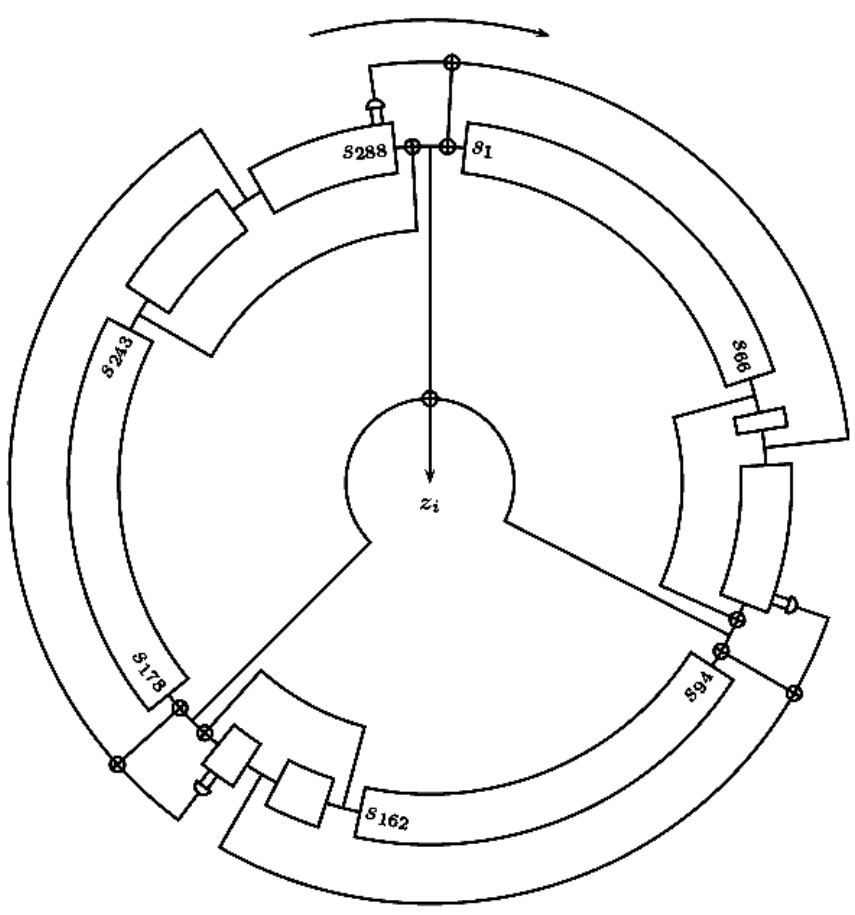
$t_3 \leftarrow t_3 + s_{286} \cdot s_{287} + s_{69}$

$(s_1\ s_2 \ldots s_{93}) \leftarrow (t_3\ s_1 \ldots s_{92})$

$(s_{94}\ s_{95} \ldots s_{177}) \leftarrow (t_1\ s_{94} \ldots s_{176})$

$(s_{178}\ s_{279} \ldots s_{288}) \leftarrow (t_2\ s_{178} \ldots s_{287})$

end for



Grain v.1

Martin Hell,
Thomas Johansson
Lund University, Sweden
Willi Meier
FH Aargau, Switzerland

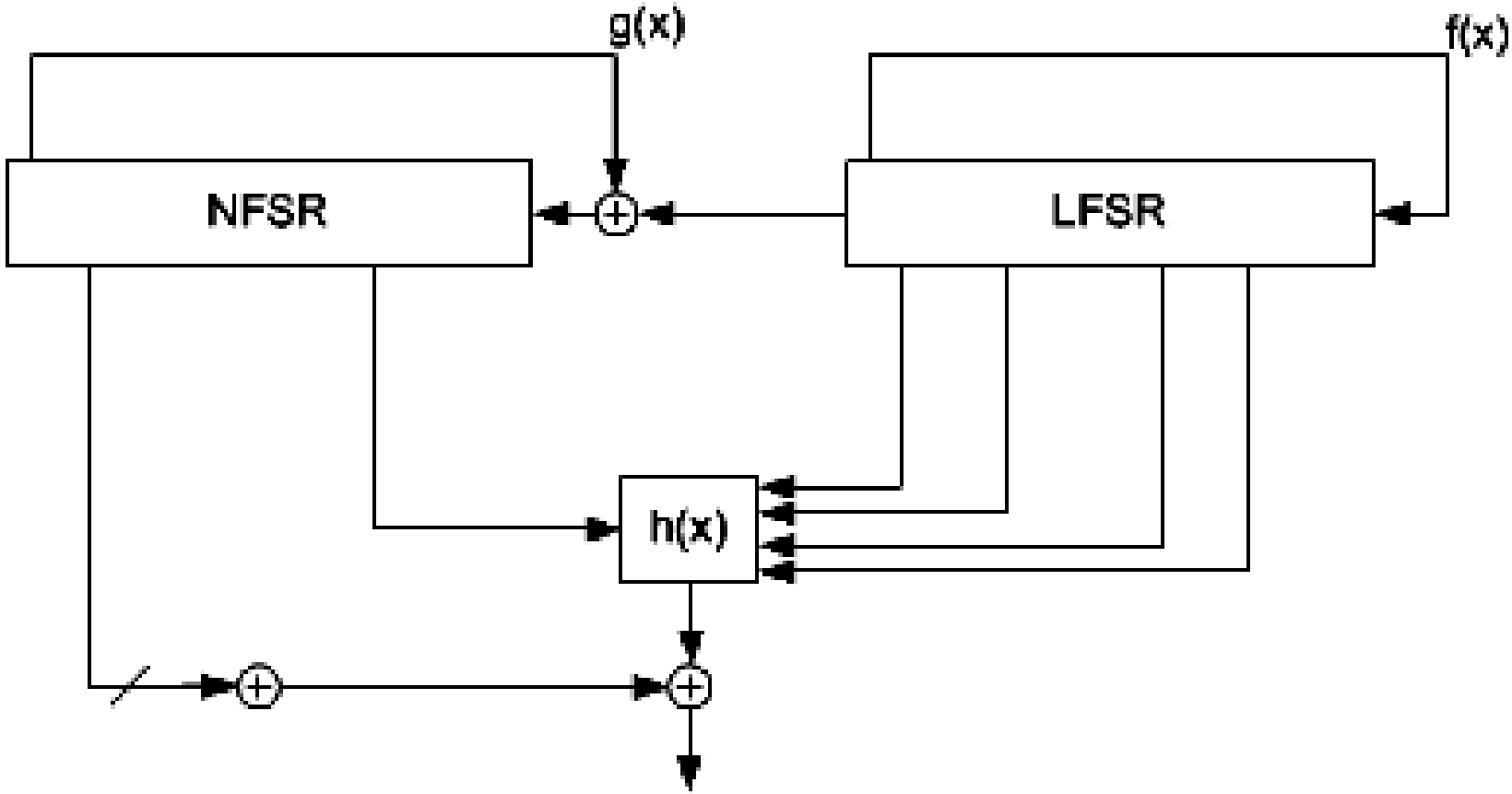
Grain v.1

Работа алгоритма определяется 80-битным секретным ключом и 64-битным IV.

Внутреннее состояние соответствующего автомата определяется 160 битами:
80-битный линейный регистр сдвига и
80-битный нелинейный регистр сдвига.

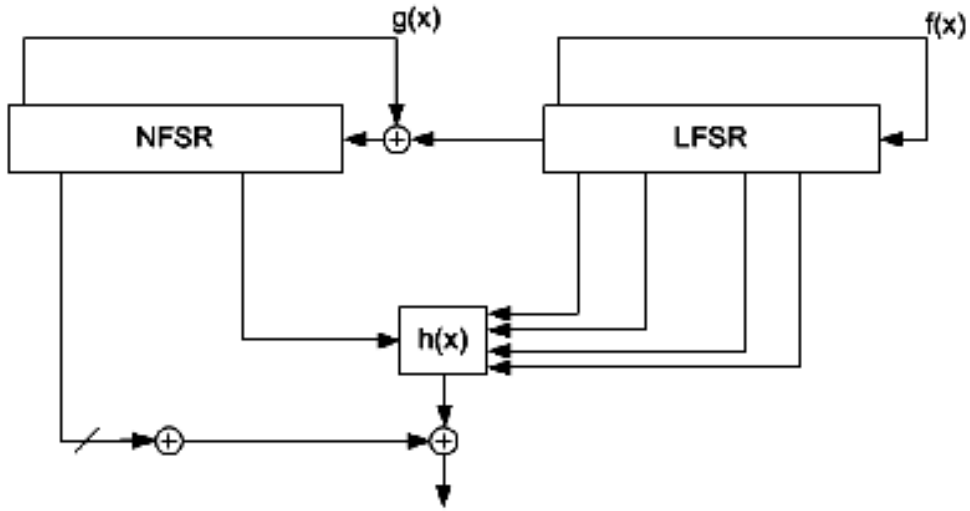
Выходом является битовая последовательность, определяемая как функция от съемов с обоих регистров.

Grain v.1



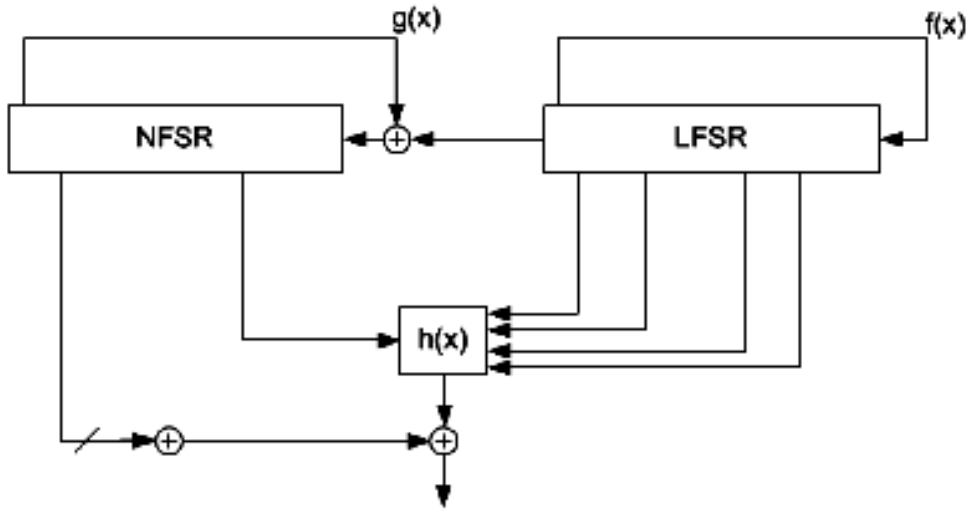
Grain v.1

$$s_{i+80} = s_{i+62} + s_{i+51} + s_{i+38} + s_{i+23} + s_{i+13} + s_i$$



$$\begin{aligned} b_{i+80} = {} & s_i + b_{i+62} + b_{i+60} + b_{i+52} + b_{i+45} + b_{i+37} + b_{i+33} + b_{i+28} \\ & + b_{i+21} + b_{i+14} + b_{i+9} + b_i + b_{i+63} \cdot b_{i+60} + b_{i+37} \cdot b_{i+33} \\ & + b_{i+15} \cdot b_{i+9} + b_{i+60} \cdot b_{i+52} \cdot b_{i+45} + b_{i+33} \cdot b_{i+28} \cdot b_{i+21} \\ & + b_{i+63} \cdot b_{i+45} \cdot b_{i+28} \cdot b_{i+9} + b_{i+60} \cdot b_{i+52} \cdot b_{i+37} \cdot b_{i+33} \\ & + b_{i+63} \cdot b_{i+60} \cdot b_{i+21} \cdot b_{i+15} + b_{i+63} \cdot b_{i+60} \cdot b_{i+52} \cdot b_{i+45} \cdot b_{i+37} \\ & + b_{i+33} \cdot b_{i+28} \cdot b_{i+21} \cdot b_{i+15} \cdot b_{i+9} + b_{i+52} \cdot b_{i+45} \cdot b_{i+37} \cdot b_{i+33} \cdot b_{i+28} \cdot b_{i+21} \end{aligned}$$

Grain v.1



$$h(x) = x_1 + x_4 + x_0x_3 + x_2x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4$$

$$x_0 = s_{i+3},\ x_1 = s_{i+25},\ x_2 = s_{i+46},\ x_3 = s_{i+64},\ x_4 = b_{i+63}$$

$$z_i = \sum_{k \in \mathcal{A}} (b_{i+k} + h(s_{i+3}, s_{i+25}, s_{i+46}, s_{i+64}, b_{i+63}))$$

$$\mathcal{A} = \{1, 2, 4, 10, 31, 43, 56\}$$

Традиции живут !

Традиции живут !

или консерватизм побеждает ?

Основные направления в разработке поточных шифров

- Разработка сверхскоростных программно-ориентированных шифров
- Разработка шифров для аппаратной реализации при различных ограничениях.
- Разработка самосинхронизирующихся поточных шифров.
- Разработка механизмов аутентификации для поточных шифров.

THE END