

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ, СТАТИСТИКИ И ИНФОРМАТИКИ (МЭСИ)

А.В. Бабаш

**СИНТЕЗ ШИФРУЮЩИХ
АВТОМАТОВ**

Монография

Москва, 2014

УДК 004
ББК 32.81
Б 12

Автор: д.ф.-м.н., профессор кафедры Информационной безопасности НИУ ВШЭ Бабаш А.В.

СИНТЕЗ ШИФРУЮЩИХ АВТОМАТОВ. – М.: НИУ ВШЭ; МЭСИ, 2014. – 257 с.

Монография знакомит читателей с теоретико-автоматными методами синтеза защиты информации.

Рецензенты:

Баранова Е.К. – доцент кафедры Информационной безопасности и программной инженерии Российского государственного социального университета;

Хорев П.Б. – канд. тех. наук, доцент, профессор кафедры Информационные системы МГТУ «СТАНКИН»

Все права защищены. Никакая часть этой книги не может быть воспроизведена в любой форме или любыми средствами, электронными или механическими, включая фотографирование, магнитную запись или иные средства копирования или сохранения информации без разрешения авторов.

Монография обсуждена и рекомендована к печати на заседании кафедр информационной безопасности МЭСИ и НИУ ВШЭ.

ISBN 978-5-7764-0858-8

© Бабаш А.В., 2014
© НИУ ВШЭ, 2014
© МЭСИ, 2014

СОДЕРЖАНИЕ

Введение	7
Определения, обозначения и сокращения.....	10
Глава 1. Классы автоматов и операции над автоматами.....	13
1.1. Автономный линейный регистр сдвига.....	13
1.2. Неавтономный линейный регистр сдвига.....	13
1.3. Неавтономный регистр сдвига	13
1.4. Проходная линия задержки	14
1.5. Шифрующий автомат.....	14
1.6. Операции над автоматами.....	15
Глава 2. Неотличимость состояний автоматов	17
2.1. Основные понятия	17
2.2. Неотличимость состояний перестановочных автоматов	19
2.3. Гомоморфизмы автоматов	24
Глава 3. Неотличимость входных слов автоматов.....	27
3.1. Автономность автоматов	27
3.2. Степени перестановочных автоматов	27
3.3. Псевдоавтономность перестановочных автоматов	30
3.4. Слабая автономность автоматов	36
3.5. Слабый гомоморфизм автоматов	40
Глава 4. Декомпозиция автоматов	44
4.1. Разбиения и покрытия множества. Примеры.....	44
4.2. Фактор-автомат. Покрытие автомата.....	46
4.3. Параллельное соединение автоматов	48
4.4. Последовательное соединение автоматов.....	50
Глава 5. Периодичность функционирования конечных автоматов	57
5.1. Вспомогательное почти тривиальное утверждение	57
5.2. Основные теоретико-автоматные обозначения.....	58
5.3. Оценка периодов последовательностей состояний автомата при заданной периодической входной последовательности.....	59
Глава 6. Гомоморфизмы неавтономных двоичных регистров сдвига	61
6.1. Основные понятия	61
6.2. Теорема А.Я. Прососова.....	62
6.3. Теорема В.А. Башева	64
6.4. Обзор по работе В.И. Солодовникова «Гомоморфизмы двоичных регистров сдвига» [20]	65
Глава 7. Верхняя оценка степени различимости связных перестановочных автоматов с заданным диаметром	73
7.1. Формулировка основных результатов	73
7.2. Доказательство основной оценки.....	73
7.3. О роли диаметра перестановочного связного приведенного автомата в его оценки степени различимости.....	75
7.4. Доказательство достижимости полученной оценки степени различимости.....	82

Глава 8. Неотличимость состояний перестановочных, аффинных и автономных нелинейных векторных автоматов	91
8.1. Основные понятия	91
8.2. Неотличимость состояний перестановочных автоматов	93
8.3. Оценки вероятности k -неотличимости двух случайно и равновероятно выбранных состояния автомата.....	97
8.4. Неотличимость состояний n -й степени перестановочного автомат	100
8.5. Неотличимость состояний аффинных автоматов	101
8.6. Неотличимость аффинных автоматов	104
8.7. Неотличимость состояний автономных векторных нелинейных автоматов	105
Глава 9. Неотличимость состояний автономного последовательного соединения перестановочных автоматов	108
9.1. Оценки числа классов неотличимых состояний автономных последовательных соединений перестановочных автоматов	108
9.2. Оценки мощностей классов неотличимых состояний автономных последовательных соединений перестановочных автоматов	116
Глава 10. Алгоритмы нахождения минимальных систем областей импримитивности группы	120
10.1. Алгоритм нахождения минимальных систем импримитивности групп подстановок (M.D. Atkinson).....	120
10.2. Новый алгоритм получения минимальных систем областей импримитивности группы подстановок	122
Глава 11. Односторонняя неотличимость состояний конечных автоматов.....	126
11.1. Понятие (Ψ, η) – неотличимости состояний автомата	126
11.2. Определение начального состояния автомата по его входному и выходному слову	127
11.3. Свойства (Ψ, η) –неотличимых состояний автомата.....	127
11.4. (η, d) – периодические выходные последовательности автономного автомата	130
11.5. G -приведенность автономного последовательного соединения автоматов.....	132
Глава 12. Сильно приведенные автоматы	134
Глава 13. Об одном подходе к линеаризации уравнений получения выходной последовательности векторного автомата.....	137
13.1. \mathfrak{Z} -размерность векторного автомата, \mathfrak{Z} -линейная размерность.....	137
13.2. Определение начального состояния векторного автомата A по его входной и выходной последовательностям	138
Глава 14. Запреты автоматов и двоичных функций.....	140
14.1. Криптографические приложения	140
14.2. Запреты автоматов	140
14.3. Запреты двоичных функций.....	144
14.4. Критерии наличия запрета двоичной функции	145
14.5. Оценки длины запрета двоичной функции	145

Глава 15. Внешне периодические автоматы.....	149
15.1. Введение.....	149
15.2. Автоматы с L-потерей информации о выходе.....	149
15.3. Критерий внешней периодичности автомата	151
Глава 16. Периодически внешне наследственные перестановочные автоматы.....	154
16.1. автоматы с L-потерей информации	154
16.2. Периодически внешне наследственные автоматы	156
16.3. Критерий внешне наследственности автомата	161
Глава 17. Периоды выходных последовательностей автомата при заданной периодической входной последовательности.....	164
17.1. Краткий обзор результатов по данной теме. Обозначения, основные понятия, вспомогательные результаты.....	164
17.2. Периоды выходных последовательностей автомата без внешне автономных состояний при входной периодической последовательности заданной полноты...	166
17.3. Периоды выходных последовательностей линейного векторного автомата при заданной входной периодической последовательности.....	171
17.4. Период внешнего функционирования автономного последовательного соединения автоматов	174
17.5. Периоды выходных последовательностей перестановочного автомата без потери информации при заданных периодических входных последовательностях	176
17.6. Периоды выходных последовательностей последовательного соединения автономного автомата с перестановочным автоматом без потери информации.....	180
Глава 18. Классы автоматов с гарантированными периодами выходных последовательностей.....	183
18.1. Необходимость построения автоматов с гарантированными периодами выходных последовательностей	183
18.2. Кодирующее устройство с конечной памятью.....	183
18.3. Полноцикловый автомат	186
18.4. Обратимый автомат.....	190
18.5. Обобщенный узел выборки.....	191
Глава 19. Классы автоматов с гарантированными параметрами подпериода выходных последовательностей.....	194
19.1. Основные обозначения и понятие подпериода последовательности.....	194
19.2. Автомат Медведева	195
19.3. Кодирующее устройство с конечной памятью.....	197
19.4. Обратимые автоматы.....	200
Глава 20. О периодичности последовательности состояний автомата, отвечающей его начальному состоянию и входной периодической последовательности. Приближенные периоды последовательности состояний автомата.....	201
20.1. Введение, вспомогательные обозначения, понятия и результаты.....	201
20.2. Нижние оценки мер приближенных периодов последовательностей состояний автомата, отвечающих его начальным состояниям и входным смешанно-периодическим последовательностям	205
20.3. Нижние оценки мер приближенных периодов выходных последовательностей регистров сдвига, отвечающих его начальным состояниям и входным смешанно-периодическим последовательностям	208

Глава 21. Приближенные периоды выходных последовательностей полноциклового автомата, представимого последовательным соединением автономного автомата с неавтономным перестановочным автоматом	210
21.1. Полноцикловое последовательное соединение автоматов.....	210
21.2. Полноцикловое последовательное соединение автономного автомата С перестановочным коммутируемым автоматом	212
21.3. Класс функций выхода полноциклового последовательного соединения автономного автомата с перестановочным коммутируемым автоматом.....	213
21.4. Автономное последовательное соединение автоматов со свойством принудительного восстановления состояния второго автомата.....	214
Глава 22. G-Изопериод выходной последовательности автономного последовательного соединения автоматов.....	219
22.1. Основные понятия и предварительные результаты	219
22.2. Изопериод последовательности внешнего функционирования перестановочного автомата при заданной входной периодической последовательности	222
22.3. Изопериоды полноциклового автомата, представимого последовательным соединением двух автоматов.....	223
22.4. Изопериоды последовательного соединения автоматов с выходным алфавитом – группой	226
Глава 23. Оценки параметров обобщенной периодичности выходных последовательностей некоторых полноцикловых автоматов с выходным алфавитом, являющимся группой	228
23.1. Основные понятия, постановка задачи.....	228
23.2. σ -периоды последовательности $A^H(P^1)$ для стабильных слева (справа) бинарных отношений на G	230
23.3. Оценки мер приближенных σ -периодов последовательности $A^H(P^1)$ для стабильных слева (справа) бинарных отношений на группе G	232
23.4. Примеры стабильных слева (справа) бинарных отношений на группе G	238
23.5. φ -периоды последовательности $A^H(P^1)$ для автоморфизмов φ группы G	239
23.6. Оценки мер приближенных φ -периодов последовательности $A^H(P^1)$ для автоморфизмов группы	241
Глава 24. Классы векторных автоматов с гарантированными периодами выходных последовательностей при заданной входной периодической последовательности	245
24.1. Основные понятия. Вспомогательные результаты	245
24.2. Способ построения векторного автомата с гарантированным выходным периодом на основе оценки его слабой автономности	247
24.3. Способ построения векторного автомата с гарантированным выходным периодом на основе нахождения его сильно различимы входных слов.....	250
24.4. Пример синтеза векторного нелинейного автомата с гарантированным выходным периодом.....	253
Список использованных источников.....	256

Введение

Монография посвящена теоретико-автоматному подходу к синтезу криптографической защиты информации. Обобщение и универсальность изложения методов синтеза шифраппаратуры достигается выбором теоретико-автоматного языка. Одновременно, постановка задач криптографической защиты в терминах теории автоматов и их решения существенно расширили классическое содержание теории автоматов.

Шифры могут описываться моделями автоматов. Так входной последовательностью (входным словом) автомата является открытый текст, подлежащий шифрованию. Выходной последовательностью является шифрованный (зашифрованный) текст. Ключами являются компоненты начальных состояний и/или функции переходов и выходов автомата. В блочных шифрах открытый текст трактуется как начальное состояние автомата, шифрованный текст как заключительное состояние автомата, в которое он приходит под воздействием последовательности раундовых ключей. Управляющие блоки шифров предварительного шифрования моделируются автономными автоматами. Для обеспечения реверсивности устройств шифрования требуют взаимную однозначность частичных функций переходов автомата, моделирующего данное устройство. То есть требуется изучение так называемых перестановочных автоматов. Учитывая криптографическую направленность приводимых теоретико-автоматных утверждений и их приложение, мы называем автоматы с изучаемыми свойствами шифрующими автоматами.

В монографии представлена методика оценки периодов и приближенных периодов выходных последовательностей автоматов при заданных начальных состояниях и входных периодических последовательностях. Решаются задачи, связанные:

- с неотличимостью состояний перестановочных автоматов и их слабой автономностью;
- с запретами автоматов и двоичных функций;
- с оценкой периодов выходных последовательностей конечных автоматов;
- с оценкой приближенных периодов выходных последовательностей автоматов;
- с оценками мер приближенных периодов выходных последовательностей автоматов, моделирующих поточные шифры.

Представлены следующие классы автоматов:

- автоматы без потери информации;
- перестановочные автоматы;
- автоматы без внешне автономных состояний;
- автономные последовательные соединения автоматов;
- линейные векторные автоматы;
- автоматы Медведева;
- кодирующие устройства с конечной памятью;
- обратимые автоматы;
- полноцикловые автоматы.

Цель монографии состоит в разработке методов синтеза шифрующих автоматов, связанных с:

- описанием новых методов оценки количества эквивалентных ключей шифров, основанных на представлении шифрсистемы или ее отдельного блока конечным автоматом;
- оценками мощностей классов неотличимых состояний автономных последовательных соединений перестановочных автоматов, моделирующих шифры предварительного шифрования;
- с описанием новых методов оценки периодов выходных последовательностей конечных автоматов, моделирующих шифры предварительного шифрования. Другими словами, данная цель состоит в нахождении новых классов дискретных устройств с гарантированными периодами выходных псевдослучайных последовательностей;
- с получением методики оценки мер приближенных периодов выходных последовательностей конечных автоматов, моделирующих шифры предварительного шифрования.

Для класса перестановочных автоматов указаны новые алгоритмы доказательства их приведенности. Разработаны новые способы проверки наличия у автоматов автономных и слабо автономных состояний. Приведены доказательства верхних оценок сложности таких алгоритмов.

Указаны новые методы доказательства приведенности автоматов из следующих классов: перестановочных, аффинных и автономных нелинейных векторных автоматов, автономного последовательного соединения перестановочных автоматов. При этом даны удобные для применения в криптографической практике методы оценки числа неэквивалентных ключей шифров построенных по классической схеме – управляющий блок и шифрующий блок (число классов неотличимых состояний автономных последовательных соединений перестановочных автоматов и оценки их мощностей. Приведенный в работе алгоритм нахождения областей импримитивности групп подстановок, заданных системой образующий элементов более эффективен, чем известные ранее и позволяет для ряда шифрсистем применять новый способ доказательства отсутствия в них эквивалентных ключей. Дело в том, что нетривиальная система классов эквивалентных ключей в этих шифрсистемах является и некоторой системой областей импримитивности группы подстановок. Полученная оценка длины запрета $n^2 2^{3n}$ произвольной двоичной функции говорит о намного меньшей трудоемкости известного метода распознавания закона функционирования проходной линии задержки с неизвестной функцией выхода, основанного на наличии запретов у данного криптографического узла. Описаны методы построения новых классов автоматов с гарантированными периодами их выходных последовательностей. Так, в частности, найдены условия кратности периодов выходных последовательностей автоматов из построенных классов периода входной последовательности. Эти классы таковы: автоматы без потери информации, перестановочные автоматы, автоматы без внешне автономных состояний, автономные последовательные соединения автоматов, линейные векторные автоматы, автоматы Медведева, кодирующие устройства с конечной памятью, обратимые автоматы.

Введены понятия:

- меры приближенного периода периодической последовательности элементов, отражающее Хэмминговую близость последовательности к периодической последовательности заданного периода;
- изопериода периодической последовательности элементов;
- σ -периода периодической последовательности элементов.

Приведены:

- оценки приближенных периодов выходных последовательностей полноциклового автомата, представимого последовательным соединением автономного автомата с неавтономным перестановочным автоматом;
- оценки изопериода и σ -периода последовательностей специальных автоматов, моделирующих получение суммарных шифров поточных шифров.

Приведенные алгоритмы и методы являются новыми и более эффективными, чем ранее известные.

Полученные результаты являются фундаментом для построения шифрующих автоматов с гарантированными периодами их управляющих и результирующих гамм. Они могут быть использованы в криптографической практике. Одновременно эти результаты являются основой для построения приближенных моделей автоматов и построения на их основе новых методов криптографического анализа и синтеза.