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»

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

ISBN 978-5-7764-0858-8

СОДЕРЖАНИЕ

Введение

Монография посвящена теоретико-автоматному подхода 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-автоматых 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 отсутствие 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 периоду 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.