

Бабенко Л. К.
Ищукова Е. А.
Сидоров И. Д.

ПАРАЛЛЕЛЬНЫЕ АЛГОРИТМЫ

ДЛЯ РЕШЕНИЯ ЗАДАЧ
ЗАЩИТЫ ИНФОРМАЦИИ

Иркутск: ИКИН-Телеком



Бабенко Л. К.
Ищукова Е. А.
Сидоров И. Д.

ПАРАЛЛЕЛЬНЫЕ АЛГОРИТМЫ

ДЛЯ РЕШЕНИЯ ЗАДАЧ
ЗАЩИТЫ ИНФОРМАЦИИ

Москва
Горячая линия – Телеком
2014

УДК 004.056.5:519.688

ББК 32.973.2-018.2

Б12

Рецензенты: зав. кафедрой Защиты информации МФТИ, доктор техн. наук, профессор *В. А. Конявский*; научный руководитель ЮР РУНЦ ИБ Южного федерального университета, доктор техн. наук, профессор *О. Б. Макаревич*

Бабенко Л. К., Ищукова Е. А., Сидоров И. Д.

Б12 Параллельные алгоритмы для решения задач защиты информации. – М.: Горячая линия–Телеком, 2014. – 304 с., ил. ISBN 978-5-9912-0426-2.

Кратко представлены основные составляющие современных криптографических систем: симметричные алгоритмы шифрования, асимметричные алгоритмы шифрования, функции хэширования. Основной упор сделан на рассмотрение практической возможности применения существующих способов анализа современных криптосистем с целью оценки их криптографической стойкости. В работе рассмотрен целый ряд параллельных алгоритмов, основанных на различных методах анализа. В качестве примеров приведены способы реализации разработанных алгоритмов с использованием двух наиболее распространенных технологий: с использованием интерфейса передачи данных MPI для организации распределенных многопроцессорных вычислений и технологии CUDA, основанной на использовании графических вычислений. Книга снабжена множеством наглядных примеров и иллюстраций. Впервые описаны подходы к разработке параллельных алгоритмов, ориентированных на программную реализацию, и предназначенных для решения задач в области информационной безопасности.

Для специалистов в области информационной безопасности, реализующих известные методы анализа зашифрованных данных с применением параллельных вычислительных систем.

ББК 32.973.2-018.2

Адрес издательства в Интернет WWW.TECHBOOK.RU

Научное издание

**Бабенко Людмила Климентьевна, Ищукова Евгения Александровна,
Сидоров Игорь Дмитриевич**

Параллельные алгоритмы для решения задач защиты информации

Монография

Редактор Ю. Н. Чернышов
Компьютерная верстка Ю. Н. Чернышова
Обложка художника О. В. Карповой



Издание осуществлено при финансовой поддержке Российского фонда фундаментальных исследований по проекту № 14-07-07002, не подлежит продаже

Подписано в печать 21.05.14. Формат 60×90 16. Усл. печ. л. 19. Тираж 250 экз.

ISBN 978-5-9912-0426-2 © Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидоров, 2014

© Научно-техническое издательство «Горячая линия–Телеком», 2014

Оглавление

Введение	3
1. Задачи защиты информации, для решения которых требуются параллельные вычисления.....	5
1.1. Введение в криптографию	5
1.2. Симметричные алгоритмы шифрования	7
1.2.1. Алгоритм шифрования DES	7
1.2.2. Алгоритм ГОСТ 28147-89	12
1.2.3. Стандарт AES.....	17
1.3. Анализ симметричных алгоритмов шифрования.....	26
1.3.1. Метод полного перебора.....	28
1.3.2. Метод встречи посередине.....	30
1.3.3. Линейный криптоанализ	31
1.3.4. Дифференциальный криптоанализ.....	32
1.3.5. Алгебраический анализ	38
1.3.6. Анализ стандарта AES	40
1.3.7. Слайдовая атака	43
1.3.8. Парадокс дней рождений и его роль в задачах криптоанализа	46
1.4. Асимметричные алгоритмы шифрования	48
1.4.1. Алгоритм RSA	49
1.5. Методы анализа асимметричных криптосистем.....	50
1.5.1. Метод базы разложения	52
1.5.2. Логарифмирование в простом поле методом решета числового поля	53
1.6. Функции хэширования	55
1.6.1. Функция хэширования SHA	57
1.6.2. Функция хэширования нового поколения Skein.....	58
1.7. Методы анализа современных функций хэширования.....	75
1.7.1. Методы, не зависящие от алгоритма преобразования	76
1.7.2. Методы, основанные на уязвимости алгоритма преобразования хэш-функции.....	77
2. Основы параллельного программирования. Основные технологии параллельного программирования	81
2.1. Основные типы архитектур высокопроизводительных вычислительных систем.....	81
2.1.1. Классификация Флинна	82

2.1.2. Классификация многопроцессорных систем	86
2.2. Особенности программирования параллельных вычислений	88
2.2.1. Основные модели параллельного программирования	90
2.2.2. Распределение данных при решении задач защиты информации.....	91
2.3. Оценка эффективности разработанных параллельных программ.....	95
2.3.1. Теоретические основы оценки эффективности параллельных алгоритмов.....	95
2.3.2. Закон Амдала.....	96
2.4. Современные технологии параллельного программирования	97
3. Введение в параллельное программирование с использованием MPI	99
3.1. Общие сведения об «Интерфейсе передачи данных» ..	99
3.2. Обзор пакетов программ для работы с MPI.....	100
3.3. Основные функции обмена данными с помощью MPI.	102
3.3.1. Базовые функции	103
3.3.2. Двухточечный обмен.....	104
3.3.3. Функции для глобального взаимодействия и синхронизации	105
4. Технология CUDA.....	107
4.1. История вычислений на графических ускорителях ...	107
4.2. Архитектура CUDA. Мультипроцессоры.....	109
4.3. CUDA Runtime API и CUDA Driver API.....	110
4.4. Вычислительная модель. Потoki, блоки, варпы.....	110
4.5. Модель памяти.....	111
4.6. Расширения языка	112
4.7. Схема программы на CUDA.....	113
4.8. Пример программы на CUDA.....	113
4.9. Набор инструментов разработчика — CUDA Toolkit, CUDA SDK.....	115
4.9.1. Отладчик Parallel Nsight	117
4.9.2. Ресурсы для разработчиков CUDA.....	117
5. Параллельные алгоритмы в современных задачах защиты информации.....	118
5.1. Задача нахождения простых чисел в заданном диапазоне	118
5.2. Задача разложения произведения на простые сомножители	125

5.2.1. Первый вариант решения	125
5.2.2. Второй вариант решения	132
5.3. Параллельные алгоритмы решета числового поля для решения задачи дискретного логарифмирования	136
5.3.1. Алгоритм параллельного просеивания	136
5.3.2. Разработка алгоритма параллельного гауссова исключения	143
5.3.3. Гауссово исключение	144
5.3.4. Реализация метода базы разложения с помощью разработанных алгоритмов	150
5.3.5. Реализация метода решета числового поля с помощью разработанных алгоритмов	151
5.3.6. Ускорение решения задачи дискретного логарифмирования с помощью предвычислений	152
5.4. Параллельные алгоритмы дискретного логарифмирования в группе точек эллиптической кривой	154
5.4.1. Метод «Встреча посередине»	154
5.4.2. Метод «встреча на случайном дереве»	154
5.4.3. Анализ методов дискретного логарифмирования на эллиптической кривой	155
5.4.4. Распределение базы точек между процессами	156
5.4.5. Планирование взаимодействия процессов в топологии «полносвязный граф»	157
5.4.6. Разработка параллельного алгоритма дискретного логарифмирования методом встречи посередине	159
5.4.7. Разработка параллельного алгоритма дискретного логарифмирования методом встречи на случайном дереве	168
5.4.8. Возможность предвычислений	171
5.5. Дифференциальный криптоанализ алгоритма шифрования DES	177
5.6. Алгоритм поиска наиболее вероятных характеристик для проведения дифференциального криптоанализа алгоритма ГОСТ 28147-89	197
5.6.1. Трудоемкость перебора	203
5.6.2. Организация межпроцессных взаимодействий	205
5.7. Пример генерации радужных таблиц на CUDA	207
5.7.1. Описание метода радужных таблиц	207
5.7.2. Вероятность успешного поиска с помощью радужной таблицы	209
5.7.3. Описание используемой обратной функции	210
5.7.4. Формат данных для хранения хеш-таблиц	211
5.7.5. Листинг основных модулей программы, предназначенной для запуска на архитектуре CUDA	211
Литература	222

Приложение А. Руководство по использованию MPICH	225
Приложение Б. Основные функции, используемые в стандарте MPI	273
Список основных сокращений и обозначений	299