Введение

Ключевой задачей защиты информации является создание стойких алгоритмов шифрования. В современной криптографии шифры по принципу построения и использования секретного ключа разделяют на симметричные и асимметричные. Любой разрабатываемый алгоритм шифрования подвергается тщательному анализу с целью выявления его слабых мест и возможности взлома. Для того чтобы иметь возможность оценить стойкость используемого шифра, необходимо наличие эффективных алгоритмов анализа.

На сегодняшний день существует довольно много различных методов анализа симметричных блочных шифров, основанных на различных подходах. Среди них можно выделить несколько основных направлений. Метод линейного анализа основан на построении системы эффективных статистических аналогов. Накопление статистики с использованием данной системы аналогов позволяет предположить значения битов секретного ключа. Метод дифференциального анализа и его производные — метод невозможных дифференциалов, бумеранг-атака — основаны на прослеживании изменения несходства между двумя текстами при их прохождении через раунды шифрования. Алгебраические методы анализа основаны на построении и решении системы линейных уравнений от многих переменных, полностью описывающих схему шифрования. Метод слайдовой атаки предназначен для анализа гомогенных шифров или шифров с некоторой степенью самоподобия. Для таких шифров рассматривается возможность сопоставления двух процессов шифрования с запаздыванием на один или несколько раундов.

Для асимметричных криптосистем также существует достаточно большое разнообразие методов. Среди них наиболее известны такие методы, как метод Гельфонда, «giant step-baby step», метод встречи на случайном дереве, метод базы разложения, метод решета числового поля, метод Ферма, метод непрерывных дробей, метод квадратичного решета и др. Однако, если при анализе симметричных криптосистем различные методы используют различные приемы, такие как линеаризация, рассмотрение пар текстов, составление систем переопределенных уравнений, то при анализе асимметричных криптосистем все методы сводятся к решению двух задач различными способами — задачи дискретного логарифмирования и

задачи факторизации больших чисел. С появлением мощных вычислительных ресурсов задача анализа асимметричных криптосистем превратилась из чисто теоретической в практическую. При этом многие из вышеуказанных методов поддаются распараллеливанию, а значит, могут работать в несколько раз быстрее при использовании соответствующих вычислительных средств.

Одним из способов повышения производительности при анализе различных криптосистем является использование распределенных многопроцессорных вычислений (РМВ) для ускорения процесса анализа и скорейшего получения результата. Применение РМВ возможно как при криптоанализе симметричных блочных шифров, так и при использовании методов анализа современных асимметричных криптосистем.

В монографии освещаются основные проблемы современной системы защиты информации в области криптоанализа. При этом отдельное внимание уделяется вопросом возможности применения высокопроизводительных распределенных вычислений для ускорения вычислительного процесса. Книга организована следующим образом. В первом разделе рассматриваются основные алгоритмы симметричного и ассиметричного шифрования, современные функции хэширования, а также основные методы анализа, связанные с оценкой уязвимостей рассматриваемых криптосхем. При рассмотрении криптоалгоритмов и методов их анализа отдельный упор делается на возможность применения РМВ для сокращения времени анализа. Во втором разделе рассматриваются основные современные типы параллельных вычислительных архитектур. Особое внимание уделяется вопросам распределения данных для распределенных вычислений, а также вопросам оценки эффективности разработанных параллельных алгоритмов. В третьем разделе приводятся краткие сведения об интерфейсе передаче данных MPI, его основных функциях и способах межпроцессного взаимодействия. В четвертом разделе описывается архитектура CUDA и возможность ее использования для распределенных многопроцессных вычислений. Наконец, в пятом разделе рабобраны подробные решения основных задач современной защиты информации, описаны детальные алгоритмы и приведены листинги программ с подробными комментариями. В приложениях даны подробные инструкции по установке, настройке и работе с пакетом программ MPICH 1.2.5, а также подробное описание библиотечных функций MPI.