ПРИНЦИПЫ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ ПРОГРАММНЫХ БИБЛИОТЕК

Агиевич С. В.

БГУ, НИИ прикладных проблем математики и информатики,
Минск, Беларусь, e-mail: agievich@bsu.by

Криптографические программные библиотеки должны не только точно и эффективно реализовывать криптографические алгоритмы и протоколы, но и соответствовать дополнительным принципам безопасности. В докладе рассматриваются принципы построения библиотеки Bee2, разработанной автором. В библиотеке реализованы алгоритмы и протоколы национальных криптографических стандартов (СТБ 34.101.31, 45, 47, 60, 66).

Переносимость. Библиотека написана на языке Си, без ассемблерных вставок и поэтому компилируется практически на любой аппаратно-программной платформе.

Контроль памяти. В низкоуровневые функции передаются указатели на память, в которой размещаются состояния алгоритмов / протоколов и локальные переменные. Память может содержать критические объекты (ключи), и поэтому взята под контроль. Память выделяется только в высокоуровневых функциях и только одним блоком: в нем размещаются и состояние, и стек всех подчиненных функций. Блок может защищаться от попадания в файл подкачки. При завершении работы с блоком его очистка выполняется так, что не может показаться бесполезной оптимизатору, и он ее не исключит из кода библиотеки.

Регуляризация. В Bee2 реализуется программа полной регуляризации. Регуляризация состоит в отказе от ветвлений, условия которых определяются критическими данными. Отказ от ветвлений блокирует атаки, основанные на замерах времени или питания.

Предусловия и ожидания. Выделены предусловия – они названы ожиданиями, – проверить которые вычислительно трудно: простота числа, неприводимость многочлена, корректность эллиптической кривой. Функции не полагаются на безусловное выполнение ожиданий и корректно работают даже при их нарушении

Интерфейсы. Высокоуровневые функции объединяются в связки. Функции связки используют общее состояние и стек, они похожи на методы класса C++. В необходимых случаях объявляются ожидания относительно последовательности вызовов функций связки.

Алгоритмы. Большое внимание уделено выбору оптимальных арифметических алгоритмов. Разработаны новые алгоритмы арифметики больших чисел.

Алгебраическая абстракция. Работа с алгебраическими структурами реализована через достаточно общие интерфейсы. Например, интерфейс `qr` описывает работу с абстрактным кольцом вычетом по модулю его идеала. Интерфейс `qr` инстанциируется многими способами: `zm` – кольцо вычетов целых чисел, `pp` – кольцо многочленов, `gfp` – простое поле из $p > 2$ элементов, `gf2` – поле характеристики 2.