Использование параллельных вычислений при реализации криптопримитивов

Е.Г. Качко

Рассмотрены вопросы оптимизации криптографических алгоритмов с учетом Стандарта FIPS PUB 186 -3, принятого в июне 2009 года с помощью параллельных вычислений. Рассмотрены методы параллелизации модульного возведения в степень для многоядерных процессоров.

Вновь принятый Стандарт FIPS PUB 186 – 3 определяет требования и алгоритмы генерации параметров, ключей, создания и проверки цифровой подписи для несимметричных методов: DSA, ECDSA и RSA. Ранее исследовано использование параллельных вычислений при генерации параметров, ключей и цифровой подписи для метода RSA в соответствии с черновым вариантом этого Стандарта. При этом предполагалось, что все базовые операции будут выполняться последовательно. В данной работе рассмотрены способы распараллеливания базовой операции несимметричной криптографии – модульное возведение в степень. Далее будет продолжено исследование для других базовых операций.

Для выполнения операции возведения в степень традиционно используется двоичный метод, основанный на представлении полинома в виде схемы Горнера. Данный метод обеспечивает эффективные вычисления для одноядерных процессоров и не допускает распараллеливания. Общее число операций, которое требуется для вычислений двоичным методом, составляет $K_1 = (n)_{sq} + (n/2)_{mul}$., где: mul – операции умножения, sq – операции возведения в квадрат при любом числе ядер. Использование блочного метода уменьшает общее число операций за счет предвычислений, но не позволяет выполнять параллельные вычисления.

Рассматривается несколько методов параллелизации вычислений модульного возведения в степень. В условиях двуядерного процессора теоретическое ускорение для предложенного метода составило 1,25. На рисунке представлена зависимость теоретического ускорения от числа процессоров. Как видно из рисунка, изменение числа процессоров не существенно влияет на ускорение, поэтому практическое исследование выполнено для двуядерного процессора..

Экспериментальная проверка выполнена для 2-х ядерного процессора Intel (R) Core (TM) 2 Duo CPU E6850 @ 3.00 GHz, 1.99 GB of RAM Physical Address Extension и длин модулей 1024, 2048, 3072. Предложенный метод позволяет получить гарантированное ускорение на 20- 22 % ,

Применение преобразований Монтгомери не изменяет качественных характеристик операции модульного возведения в степень для последовательного и параллельного выполнения, правда ускорение снижается от 20 до 17%. Это связано с тем, что требуются дополнительные преобразования, которые выполняются в последовательной части программы.