СЕКЦИЯ 3. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

ПАРАЛЛЕЛЬНЫЕ ВЫЧИСЛЕНИЯ ОСНОВНЫХ КРИПТОГРАФИЧЕСКИХ ОПЕРАЦИЙ В СИСТЕМАХ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Д.М. БИЛЬДЮК

Преимуществом криптосистем на эллиптических кривых является то, что при выполнении операции шифрования отсутствует очень медленная операция возведения больших чисел в степень по модулю, характерная для других криптосистем с открытым ключом (например, RSA). Базовой операцией в группе точек эллиптической кривой, определяемой конкретным уравнением, являются операции сложения и удвоения точек в аффинных координатах, связанных с модулярным умножением.

Наиболее распространенным методом при реализации модульного возведения в степень (в классических криптосистемах, например RSA) является метод Монтгомери. Реализация последнего имеет большую скорость выполнения по сравнению с другими методами умножения больших чисел и последующего вычисления остатка от деления (например, умножение по методу Карацубы и последующее вычисление остатка на основе спуска Ферма). Однако при выполнении операции модульного умножения метод Монтгомери не имеет преимуществ по скорости и его использование становиться неэффективным. Параллельная реализация указанных методов в позиционных системах счисления позволяет значительно повысить скорость выполнения базовых операций известных криптосистем с открытым ключом, но недостатки метода Монтгомери относительно эллиптических кривых сохраняются. Параллельная реализация модульного умножения по методу Монтгомери в непозиционной системе счисления на основе остаточных классов дает значительный прирост в скорости, и позволяет рассматривать указанный метод как наиболее эффективный.

Сравнительный анализ скорости выполнения базовых операций в криптосистемах с открытым ключом осуществлялся на основе технологии параллельных вычислений CUDA.

ИЕРАРХИЧЕСКАЯ СИСТЕМА УСЛОВНОГО ДОСТУПА К МУЛЬТИМЕДИЙНОМУ КОНТЕНТУ С ЗАЩИТОЙ ОТ КОАЛИЦИОННЫХ АТАК

А.А. БОРИСКЕВИЧ

В настоящее время среди пользователей глобальной сети все более востребованными становятся службы передачи мультимедийных данных. Актуальными становятся задачи организации условного доступа к платному мультимедийному контенту в глобальной сети Интернет. Система условного доступа должна обеспечивать доступ к контенту с различным качеством, при этом, учитывая среду распространения контента, система должна быть защищена от коалиционных атак.