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.

Условный доступ к мультимедийным данным с разным качеством основан на декомпозиции контента, представлении его в виде множества пакетов, селективном или полном шифровании пакетов. Шифрование пакетов может быть произведено несколькими способами. Простейший способ заключается в шифровании каждого пакета независимыми ключами. При этом множество ключей декоррелированно, что не дает возможности осуществить коалиционную атаку на ключи. Однако в этом случае лицензия, выдаваемая пользователю, должна содержать множество ключей, необходимых для расшифрования контента с заданным качеством. Количество передаваемых ключей зависит от параметров декомпозиции контента и предоставляемого уровня качества. Другим подходом к решению проблемы является использование иерархии ключей. При использовании иерархии ключей лицензия содержит только один ключ, необходимый для расшифрования контента. Нижестоящие в иерархии ключи определяются через одностороннюю хэш-функцию. Недостатком применения иерархии ключей является их подверженность коалиционным атакам при более двух типах декомпозиции и отсутствии дополнительных мер защиты.

Для организации защищенного от коалиционных атак условного доступа к мультимедийному контенту предлагается система условного доступа, основанная на модифицированной структуре иерархических ключей. Защита от коалиционных атак осуществляется за счет введения дополнительных защитных субключей и основывается на дополнении или замещении исходной иерархии ключей защищенной иерархией. При этом предлагаемая система имеет режим частичной защиты с запрещением перехода к высшим уровням качества и режим полной защиты от коалиционных атак. Режим частичной защиты обеспечивает большее быстродействие за счет незначительного увеличения структуры ключа. Данный режим может быть использован для контента с большим количеством типов и уровней декомпозиции. Режим полной защиты полностью предотвращает коалиционные атаки на секретные ключи, но требует большее количество защитных субключей и имеет меньшее быстродействие. Предлагаемая система поддерживает как полное, так и селективное шифрование контента в зависимости от требований к быстродействию и деградации качества при восстановлении контента без вышестоящих в иерархии ключей.

Гибкость разработанной системы дает возможность использовать ее для широкого спектра задач, направленных на организацию условного доступа к мультимедийному контенту в глобальной сети.

АЛГОРИТМ ГЕНЕРАЦИИ ХАОТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С УЛУЧШЕННЫМИ КРИПТОГРАФИЧЕСКИМИ ХАРАКТЕРИСТИКАМИ

А.А. БОРИСКЕВИЧ, Д.М. ШУТ

Генерация псевдослучайных последовательностей с хорошими криптографическими характеристиками является одной из важнейших задач в области защиты информации. Одной из причин использования цифровых хаотических систем для улучшения качества генераторов является простота реализации и тесная взаимосвязь между хаотическими (эргодичность, высокая чувствительность к начальным условиям/ управляющему параметру, детерминированная динамика и структурная сложность) и криптографическими свойствами (перемешивание, рассеяние, детерминированная псевдослучайность, алгоритмическая сложность).