С. Н. Кяжин, А. В. Моисеев

КРИПТОГРАФИЯ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ: СОВРЕМЕННОЕ СОСТОЯНИЕ И АКТУАЛЬНЫЕ ЗАДАЧИ

Введение

Облачные вычисления получили значительное развитие в последние годы. Действительно, эта технология очень удобна для пользователей, она предоставляет доступ к пользовательским данным в любое время в любом месте. С другой стороны, как правило, облачные ресурсы в значительной мере превосходят ресурсы, которыми обладают обычные пользователи, поэтому могут решать некоторые сложные задачи за более короткое время.

Быстрое предоставление услуг и защищенность данных от НСД делают облачные технологии привлекательными для предприятий ИТ-бизнеса.

Рассмотрим основные риски нарушения информационной безопасности в облачных вычислениях:

- доступ к данным со стороны провайдера (злонамеренный инсайдер);
- публичное разглашение данных (доступ неограниченного круга лиц);
- вынос/выемка данных или носителей из датацентра провайдера (органы, сотрудники);
- ошибки изоляции среды (доступ одного клиента облака к данным других клиентов);
- недостаточное уничтожение данных провайдером при уходе клиента или стирании данных.

Предложенные подходы к шифрованию в облачных средах:

- программные агенты на конечных точках, обращающихся к облаку;
- шлюз/прокси — виртуальный или физический;
- шифрование непосредственно в самой облачной инфраструктуре.

В связи с изложенными рисками нарушения информационной безопасности и предложенными подходами к шифрованию в облачных средах для защиты информации могут применяться различные криптосистемы с открытым ключом (схемы асимметричного шифрования и электронной цифровой подписи). Для обеспечения надежной защиты информации необходимо использование стойких криптографических алгоритмов.

С другой стороны, облачная модель должна поддерживать высокую доступность сервисов, а также удовлетворять свойству «быстрой эластичности» (rapid elasticity), а именно: вычислительные возможности должны предоставляться быстро и эластично «изменяемого объема», в ряде случаев — автоматически, для оперативного повышения масштабируемости (scale out) и быстрого освобождения для уменьшения масштабов потребления (scale in).

Чтобы обеспечить постоянный доступ пользователя к его ресурсам в облаке, необходимо поддерживать безопасные технологии передачи и хранения данных вне зависимости от возможностей клиента в настоящий момент. В частности, необходимо обеспечить конфиденциальность данных при хранении и передаче посредством шифрования.

Клиенту позволено обращаться к облаку с помощью практически любого устройства, но оно может быть не в состоянии поддерживать шифрование некоторыми алгоритмами ввиду сложности и энергоемкости их реализации. В таком случае можно использовать алгоритмы легковесной (или низкоресурсной) криптографии, стойкость которых снижается незначительно, в отличие от объема требуемых ресурсов.

1. Легковесная криптография

Основным сдерживающим фактором на пути оптимизации ИТ-инфраструктуры является вопрос о надежности защиты информации. В связи с этим возникает проблема обеспечения

безопасности компонентов структуры ОВ, а также обрабатываемых и хранящихся в облаке данных. Кроме того, существенной проблемой для многих регионов нашей страны становятся высокие требования к качеству каналов связи при использовании технологии ОВ, которые предполагают повсеместный доступ к сети Интернет.

Удобство использования и доступность данных из любой точки мира делают облачные вычисления все более популярной услугой для большого круга пользователей. Однако концентрация большого объема данных в едином пространстве создает удобную мишень для нарушителей. Поэтому при построении сред облачных вычислений стоит уделить особое внимание вопросам безопасности.

Легковесная криптография — раздел криптографии, имеющий своей целью разработку алгоритмов для применения в устройствах, которые не способны обеспечить большинство существующих шифров достаточными ресурсами (память, электропитание, размеры) для функционирования.

Наступающая эра всепроникающей вычислительной техники будет отличаться наличием многих смарт-устройств, которые в связи с жестким ограничением стоимости, характерным для массового внедрения, будут иметь ограниченные ресурсы, такие как память, вычислительная мощность и время работы от батареи. В этом случае необходимо толковать закон Мура по-другому: вместо того чтобы удваивать производительность, мы видим уменьшение в два раза цены на вычислительную мощность каждые 18 месяцев. Так как многие приложения имеют очень жесткие ограничения ресурсов, например RFID, с течением времени закон Мура будет больше задействовать такие приложения. Многие приложения будут обрабатывать такую важную информацию, как наблюдение за здоровьем или биометрические данные, поэтому спрос на криптографические компоненты, которые могут быть эффективно реализованы, сильно растет.

Разработчики легковесной криптографии сталкиваются с тремя компромиссами: безопасность, стоимость, производительность. Как правило, легко оптимизировать любые две из трех целей разработки: безопасность и экономичность, безопасность и производительность или стоимость и производительность, однако очень трудно оптимизировать все три цели разработки одновременно. Например, безопасность и высокая производительность оборудования могут быть достигнуты на конвейерах, устойчивых к побочным каналам архитектурах, тем самым появляются высокие требования к оборудованию и, как следствие, высокая стоимость. С другой стороны, можно спроектировать безопасное, недорогое оборудование с ограниченной производительностью.

Существует достаточно много реализаций легковесной криптографии, программных и аппаратных. У них разные, а иногда и противоположные характеристики. Например, перестановочный бит в аппаратной реализации практически ресурсонезависим, тогда как в программной реализации он может значительно замедлить работу. Кроме того, большая таблица подстановок часто хорошо реализуется в программном обеспечении, в то время как аппаратные реализации могут быть относительно дорогими. Наконец, различия в определении количественных показателей: для программной реализации мы сравниваем требования ОЗУ и ПЗУ, а также необходимое количество тактов, а для аппаратной реализации мы фокусируемся на требованиях размера чипа и количества тактов. Программная реализация позволяет нам приблизительно оценить потребляемую мощность, умножив время обработки на среднюю потребляемую мощность устройства.

Другое различие симметричных и асимметричных шифров в том, что последние предлагают больше функций безопасности и потому имеют разные способы применения. Симметричные шифры служат, главным образом, для проверки целостности сообщений, аутентификации объектов и шифрования, в то время как асимметричные шифры обеспечивают распределение ключей и строгое выполнение обязательств. Асимметричные шифры в вычислительном отношении гораздо более требовательны к аппаратной и программной реализации. Разрыв в производительности на

устройствах с ограниченными ресурсами, такими как 8-разрядные микроконтроллеры, огромен. Например, оптимизированный асимметричный алгоритм, такой как криптография на эллиптических кривых (ECC), работает от 100 до 1000 раз медленнее, чем стандартные симметричные шифры, такие как улучшенный стандарт шифрования (AES), алгоритм, у которого на два-три порядка выше энергопотребление. В отличие от блочных шифров, которые хорошо изучены и понятны, поточные шифры не получили особого внимания со стороны научного сообщества. Хотя этот факт в последнее время меняется, приведем поточные шифры только для сравнения. (Рост интереса к поточному шифру наблюдается в таких проектах, как eStream, в пределах European Network of Excellence в области криптографии, который нацелен на стимулирование знаний о поточных шифрах.)

Ни один из известных поточных LW-шифров (MICKEY, Trivium, GRAIN и A2U2), имеющих относительно приемлемые характеристики, не удовлетворяет требованиям в полной мере. Первые три из указанных шифров неприменимы в пассивных RFID-системах в силу индивидуальных особенностей каждого из них. Так, например, Trivium требует площадь чипа, превышающую допустимую более чем в полтора раза (3488 GE при ограничении в 2000 GE). На текущую версию шифра GRAIN может быть успешно проведена атака на связанных ключах. Что касается MICKEY, то разработчиками проверена его стойкость лишь к некоторым атакам, однако этого недостаточно для обеспечения уверенности в его надежности. Кроме того, исправления в атаке по открытому тексту для алгоритма A2U2 ставят под сомнение его конкурентоспособность.

В области блочных шифров ситуация обстоит несколько лучше. Хотя для раскрытия полным перебором ключа модифицированного алгоритма DES, одного из лучших по всем параметрам, требуются месяцы работы кластера из нескольких десятков компьютеров, на суперкомпьютере данная задача решается всего за три дня. Следовательно, подобный алгоритм стоит применять только там, где требуется краткосрочная защита или где важность защищаемых данных относительно невелика. Для реализации алгоритма необходимо 1848 GE, что является приемлемым требованием для LW-шифра.

Однако, несмотря на все достоинства описанных выше блочных шифров, и для них существуют угрозы, не позволяющие использовать их повсеместно. Они имеют определенные недостатки. Например, рассмотренные алгоритмы показывают неплохие результаты как в плане быстродействия, так и в плане экономичности, однако проведено недостаточно их исследований, что, как и в случае с поточными алгоритмами, не позволяет с должной уверенностью судить об их надежности. Другие же шифры требуют для аппаратной реализации слишком много места на чипе.

2. Криптосистемы, основанные на билинейных спариваниях

Безопасность криптосистем с открытым ключом основана на сложности решения некоторых общеизвестных математических задач, таких как, например, задача факторизации целого числа и задача дискретного логарифмирования в конечном поле. Алгоритмы решения данных задач имеют субэкспоненциальную сложность, поэтому при определенных размерах ключей их решение полагают невозможным на современном этапе развития вычислительной техники. В 90-х годах XX в. получили распространение асимметричные криптосистемы на эллиптических кривых, использующие в качестве базовой алгебраической структуры группу точек эллиптической кривой, заданной над конечным полем. Эллиптические криптосистемы получаются небольшим преобразованием схемы Эль-Гамаля, основаны на сложности решения задачи дискретного логарифмирования и обеспечивают аналогичный уровень безопасности при меньших длинах ключей.

В 2000 г. в работе Антуана Жу предложено использовать спаривание Вейля для создания новых типов криптосистем, не получающихся путем переноса на эллиптические кривые. Многие криптосистемы, использующие билинейные отображения, являются криптосистемами на основе

идентификационных данных (КСОИД), что делает их привлекательными для использования в рамках ИТ-бизнеса.

КСОИД — асимметричная криптосистема, в которой открытый ключ пользователя вычисляется известным способом на основе идентификационных данных пользователя. Главным преимуществом перед классическими асимметричными криптосистемами является упрощение инфраструктуры открытых ключей (отмена сертификатов открытых ключей). Такой подход к делу позволяет упростить различные криптосхемы, управляющие большим числом открытых ключей. Вместо того чтобы хранить огромную базу данных открытых ключей пользователей, система может хранить только их идентификационные данные (имена, адреса электронной почты и др.) и при необходимости получать открытые ключи.

В связи с описанными выше требованиями безопасности и эффективности, предъявляемыми к провайдеру услуг облачных вычислений, возможно использование КСОИД, основанных на спаривании, для защиты информации в облачных вычислениях.

Однако вычисление спаривания — достаточно трудоемкая задача, поэтому основной целью данного проекта является разработка метода оптимизации вычисления спаривания в условиях многопроцессорной вычислительной системы.

На данный момент не найдено методов эффективной реализации криптосистем, основанных на спаривании, в условиях многопроцессорной вычислительной системы, позволяющих сократить время их реализации в сравнении с однопроцессорной вычислительной системой. С другой стороны, разработка таких методов позволяет значительно расширить область применения криптографии, основанной на спаривании. А возможность построения на билинейных отображениях КСОИД делает такие криптосистемы привлекательными для использования в целях защиты информации в облачных вычислениях.

СПИСОК ЛИТЕРАТУРЫ:

1. LW-криптография: шифры для RFID-систем [Электронный ресурс]. URL: http://habrahabr.ru/post/119700 (дата обращения 15.07.2013).

2. *Косолапов Д. О.* Построение многосторонних мультилинейных алгоритмов в условиях различных моделей безопасности. Дисс. … канд. физ.-мат. наук. М., 2010.