УДК 004.056.5

КОСТЕНКО Ю. В.,
МАРКОВСКИЙ А .П.,
РУСАНОВА О .В.

МЕТОД ЗАЩИЩЕННОГО МОДУЛЯРНОГО ЭКСПОНЕНЦИРОВАНИЯ НА УДАЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

В статье предложен способ удаленного модулярного экспоненцирования в облачных системах с защитой данных и кода экспоненты. Предложенный способ позволяет разделить процедуру модулярного экспоненцирования на две составляющие, одна, меньшая часть которых выполняется пользователем, а другая, большая - в удаленных мощных вычислительных системах. Подробно описаны математические принципы предлагаемого разделения вычислений, изложена методика организации вычисления. Приведены числовые примеры удаленного защищенного вычисления экспоненты.

In this paper a method for the performing the calculations required for modular exponentiation using remote or distant computational resources. The proposed method operates by separating the procedure for modular exponentiation in two components. The first component which is computationally simple is performed on the user terminal and the second and computationally complex component, is executed on powerful cloud computational resources. The details of the proposed distributed calculation are presented. Hence, the methodology for the organization of the calculations is analyzed. The calculation is illustrated by means of a simple numerical example.

Ключевые слова: розподілені віддалені обчислення, модулярне експоненціювання, хмарні обчислення, криптографія з відкритим ключем, захищені обчислення.

Введение

Одним из наиболее значимых событий текущего тысячелетия в области информационных технологий стало появление облачных вычислений. Новая технология позволяет предоставить значительные по объёму вычислительные ресурсы для решения различных пользовательских задач. Возможность удаленного доступа к таким ресурсам существенно повышает уровень информатизации во всех сферах человеческой деятельности. Вместе с тем, развитие облачных технологий порождает ряд проблем, одной из которых может быть возможность предоставления ресурсов для решения задач, связанных со взломом протоколов криптографической защиты. Таким образом, внедрение облачных технологий объективно требует повышения уровня защищенности существующих систем защиты информации [1].

Математической основой большинства сетевых проколов криптографической защиты информации является модулярное экспоненцирование, то есть вычисление $A^E \bmod M$ [1]. Уровень защищенности этих протоколов полностью определяется разрядностью используемых в операции модулярного экспоненцирования чисел. В настоящее время в большинстве протоколов используется разрядность 2048 [2], очевидным путем повышения уровня защищенности является увеличение разрядности до 4096 или 8192. Рост разрядности имеет следствием экспоненциальное возрастание вычислительной сложности реализации сетевых протоколов защиты информации. Эта проблема становится особенно ощутимой для маломощных терминальных и мобильных устройств, поддерживающих сетевые протоколы. Выполнение на таких устройствах модулярного экспоненцирования на разрядностях, больших 2048, может привести к нарушению временных рамок работы протокола. В таком случае, актуальной становится задача повышения производительности операции модулярного экспоненцирования на маломощных терминальных и мобильных устройствах, поддерживающих протоколы криптографической защиты. Одной из её возможностей является использование удаленных вычислительных ресурсов облачных технологий. Однако для реализации этой возможности необходимым условием является организация удаленных вычислений без передачи пользовательских данных в сеть. Другими словами, при вычислении $A^E \bmod M$ необходимо учесть: M является частью открытого ключа и может передаваться в явном виде, компоненты E и A являются секретным ключом и секретными данными соответственно, и их передача по сети в явном виде должна быть исключена. Таким образом, научная

задача организации удаленного вычисления модулярной экспоненты, которая исключает передачу секретных данных, является актуальной и важной на современном этапе развития информационных технологий.

Анализ известных методов защищенной реализации модулярного экспоненцирования в открытых удаленных системах

Одним из основных недостатков облачных технологий, существенным образом ограничивающим их применение, является возможность несанкционированного доступа к данным пользователя при передаче и их обработке на удаленных вычислительных мощностях. Проблеме защиты данных пользователя в системах удаленной обработки посвящено в последние годы значительное число работ. Основная проблема состоит в том, что не существует единого подхода к защите данных в процессе их обработки. Фактически, подавляющая часть выполненных исследований решает проблему защиты данных только для отдельных классов вычислительных задач, например, для линейной алгебры, обработки изображений и т.п. [2]. Широким фронтом ведутся исследования, направленные на создание эффективной защищенной организации выполнения в открытых удаленных системах операции модулярного экспоненцирования – базовой процедуры широкого класса протоколов защиты информации [3]. Их анализ показал, что решение задачи защищенного модулярного экспоненцирования состоит в разделении вычислений на две части – одна, большая часть, выполняется на удаленных вычислительных мощностях, другая, меньшая по объему – на компьютерной системе пользователя. В качестве критериев эффективности организации удаленного вычисления модулярной экспоненты логичным представляется использовать:

– уровень защищенности, мерой которого является объем ресурсов, которые нужно затратить для восстановления секретных компонент операции по кодам передаваемых в открытую систему данных;

– соотношение числа операций выполняемых на процессоре пользователя при использовании удаленных вычислений и числа операций при условии, что все модулярное экспоненцирование осуществляется пользователем.

Последний критерий позволяет оценить возможность ускорения реализации сетевых протоколов защиты информации за счет использования возможностей современных облачных технологий без ущерба для информационной безопасности.

В работе [4] предложен метод удаленного вычисления модулярной экспоненты на основе случайного разделения кода экспоненты E на группы разрядов. Это позволяет организовать вычисление $A^E \bmod M$ в виде произведения частичных экспонент, которые могу вычисляться независимо на удаленных вычислительных мощностях облаков. Формирование произведения, то есть формирование результата $A^E \bmod M$ осуществляется пользователем. Для защиты компоненты A данных используется выполнение нескольких первых шагов экспоненцирования на компьютере пользователя.

Существенным достоинством рассмотренного метода является то, что в полной мере могут быть использованы возможности многопроцессорных удаленных систем по параллельному вычислению частичных экспонент. В работе [4] на основе теоретических и экспериментальных данных установлено, что описанный метод позволяет примерно в три раза реально повысить производительность выполнения модулярного экспоненцирования.

В работе [3] предложен метод удаленного вычисления модулярной экспоненты на основе поэтапного разложения компоненты A. Такой подход позволяет разложить задачу вычисления $A^E \bmod M$ на ряд экспонент, которые оперируют с модифицированными данными и могут также вычисляться параллельно на удаленных вычислительных мощностях. Метод позволяет примерно в 2-3 раза ускорить процесс модулярного экспоненцирования. Еще один интересный подход предложен в работе [2]. Основной акцент в этих исследованиях сделан на том, чтобы пользователь мог не только удаленно выполнить модулярное экспоненцирование в закрытом режиме, но и косвенно контролировать правильность выполненных операций.

Проведенный анализ современного состояния организации защищенной реализации модулярного экспоненцирования на открытых удаленных вычислительных системах показывает, что основным их недостатком является относительно малая эффективность в плане ускорения выполнения операции модулярного экспоненцирования.

Целью исследований является повышение эффективности использования удаленных вычислительных мощностей, предоставляемых облачными технологиями, для реализации сетевых

криптографических протоколов защиты информации.

Метод защищенного удаленного вычисления модулярной экспоненты

Для достижения поставленной цели предложен метод организации вычисления модулярной экспоненты с использованием возможностей удаленных вычислительных мощностей.

Предложенный метод вычисления $A^E \mathrm{mod} M$ предполагает, что A, E, M – n-разрядные двоичные числа, удовлетворяющие условиям $A<M$, $E<M$. Метод предусматривает нахождение пары чисел G и R таких, что $G^R \mathrm{mod} M = 1$. В большинстве сетевых протоколов защиты информации используется алгоритм *RSA*, в котором модуль M образуется путем произведения двух простых чисел p и q. Например, если $p=7$ и $q=11$, то $M=77$. Соответственно, в рамках этого примера могут быть выбраны числа $G=19$ и $R=30$, такие, что $1930 \bmod 77 = 1$. Подбор чисел G и R может производиться с использованием малой теоремы Ферма.

При необходимости вычисления $A^E \mathrm{mod} M$, например, при $1431 \mathrm{mod} 77$ ($A=14$, $E=31$, $M=77$) предлагается выполнять следующую последовательность действий:

1. Вычисляется значение $B=G \cdot A \bmod M$, в частности, в рамках рассматриваемого примера $B=19 \cdot 14 \bmod 77 = 35$.

2. Случайным образом выбирается число W, разрядность которого значительно меньше разрядности n, например $W=3$.

3. Вычисляется $V=E-W$; для рассматриваемого примера $V=28$

4. Числа B, V, M передаются в облако, где вычисляется $C=B^V \mathrm{mod} M$ и полученное значение возвращается пользователю. В рамках рассматриваемого примера в облако передаются $B=35$, $V=28$, $M=77$, где вычисляется $C=35^{28} \mathrm{mod} 14=14$ и результат – число 14, возвращается пользователю.

5. Одновременно пользователь вычисляет $F=B^{R-V} \mathrm{mod}\ M$; для рассматриваемого примера $F=352 \mathrm{mod}\ 77=70$.

6. Также пользователь независимо вычисляет $D=A^{E-R} \mathrm{mod} M$, значение которого для рассматриваемого примера равно $D=A^1 \mathrm{mod} M=14$.

7. По получении из облака значения C пользователь вычисляет значение модулярного произведения $R=C \cdot F \cdot D \bmod M$; для рассматриваемого примера это значение определяется в виде $R=14 \cdot 70 \cdot 14 \bmod 77=14$. Очевидно, что полученное значение совпадает с $14^{31} \mathrm{mod}\ 77$. Конструктивность предложенного метода может быть доказана следующим образом. Учитывая что вычисляемое в облаке значение $C=B^V \mathrm{mod} M = (G \cdot A)^V \mathrm{mod} M = (G^V \mathrm{mod} M \cdot A^V \mathrm{mod} M) \bmod M$, а вычисляемое пользователем значение F можно представить как $F=B^{R-V} \mathrm{mod} M=(G \cdot A)^{R-V} \mathrm{mod} M=(G^{R-V} \mathrm{mod} M \cdot A^{R-V} \mathrm{mod} M) \mathrm{mod} M$, то произведение R можно представить в виде $R=C \cdot F \cdot D \bmod M = (G^{V} \cdot G^{R-V}) \bmod M\ (A^V \cdot A^{R-V} \cdot A^{E-R}) \mathrm{mod}\ M = (G^R \bmod M \cdot A^E \mathrm{mod} M) \bmod M$. В силу того, что $G^R \mathrm{mod} M=1$, то $R=A^E \mathrm{mod} M$, что и требовалось доказать.

Оценка эффективности

Важнейшим элементом проведенных исследований является оценка эффективности предложенного метода. Оценивание эффективности целесообразно проводить по двум критериям:

1) Достигаемое повышение производительности выполнения операции модулярного экспоненцирования пользователем

2) Влияние на уровень защищенности передачи в открытую систему значений B, V, M.

Повышение производительности проще всего оценить путем подсчета количества операций модулярного умножения. Классический алгоритм модулярного экспоненцирования состоит в последовательной обработке каждого из n разрядов кода экспоненты. Обработка одного разряда состоит из обязательного возведения в квадрат кода предыдущего результата и модулярного умножения результата на A, если текущий бит экспоненты равен 1. Если предположить примерно равное количество единиц и нулей в коде экспоненты, то очевидно, что среднее количество операций модулярного умножения составляет $1.5 \cdot n$.

В предлагаемом методе пользователь выполняет следующие операции модулярного умножения: при вычислении $F=A^{E-W} \mathrm{mod} M$ выполняется $1.5 \cdot z$ операций модулярного умножения, где z – разрядность R-V; при вычислении $D=A^{E-W} \mathrm{mod}\ M$ выполняется $1.5 \cdot y$ операций модулярного умножения, где y – разрядность разности $U=E-W$. Согласно разработанному методу разрядность U малая, равно как и разрядность разности R-V, это означает, что число выполняемых пользователем $1.5 \cdot (z+y)$ операций модулярного умножения существенно меньше, чем $1.5 \cdot n$. В частности, на практике $n=4096$, $U=32$, $z<=32$, соответственно, при выполнении модулярного экспоненцирования полностью пользователем, число операций

модулярного умножения равно 4096·1.5, а при выполнении модулярного экспоненцирования по предложенному методу пользователю необходимо выполнить только 64·1.5 операций модулярного умножения. Таким образом, для реальной ситуации, количество операций, выполняемых пользователем, сокращается в 64 раза.

Проведенные экспериментальные исследования в целом подтвердили проведенные выше теоретические оценки: время выполнения операций модулярного экспоненцирования реально сократилось в 60 раз при разрядности операндов 4096 и в 28 раз при разрядности операндов 2048.

Для оценки уровня защищенности предлагаемого метода следует учесть, что в распоряжении потенциального злоумышленника могут находиться коды *B* и *V*. Злоумышленник знает, что код *V* отличается от кода *E* в небольшом числе разрядов (не более 32), и хотя перебор 2^{32} вариантов технически реализуем, злоумышленник лишен возможности оценки правильности выбранного варианта, поскольку он не знает кода *A*. Исходя из этого, потенциальной тактикой злоумышленника может быть подбор *A*, что требует перебора 2^{n-1} вариантов. Общее число вариантов, которые необходимо перебрать составляет 2^{n-1+z}. На практике это значение примерно равно разрядности *U* – 24095+32=24127. Перебор такого числа вариантов технически нереализуем.

Классическая задача вскрытия *RSA* методом перебора требует анализа 24096 вариантов. Предложенный метод требует 24127 вариантов, что усложняет задачу взлома и таким образом повышает уровень защищенности.

Выводы

В результате проведенных исследований предложен метод защищенного модулярного экспоненцирования на удаленных вычислительных системах. Защита компонент модулярного экспоненцирования достигается за счет специального маскирования компоненты, которая возводится в степень, а так же модификации кода экспоненты. Теоретически и экспериментально доказано, что предложенный метод позволяет за счет использования удаленных вычислительных ресурсов на порядки уменьшить время выполнения экспоненцирования. Доказано, что за счет введения маскирования предложенный метод позволяет увеличить уровень защищенности компонент модулярного экспоненцирования. Предложенный метод ориентирован в первую очередь на маломощные терминальные микроконтроллеры и мобильные устройства, поддерживающие протоколы защиты информации в сетях, поскольку позволяет значительно сократить время трудоемких операций модулярного экспоненцирования даже для больших разрядностей чисел. Проведенные исследования доказали, что для таких устройств, даже при разрядности 8192 реализация протоколов криптографической защиты не выходит за установленные временные границы.

Список литературы

1. Boroujerdi N. Cloud Computing: Changing Cogitation about Computing/ Boroujerdi N., Nazem S. // IJCSI International Journal of Computer Science Issues, – Vol. 9, – Issue 4. –2012. – No 3. – PP. 169-180.
2. Xiaofeng Chen. New Algorithms for Secure Outsourcing of Modular Exponentiations / Xiaofeng Chen, Jin Li, Jianfeng Ma, Qiang Tang, Wenjing Lou // ESORICS 2012, LNCS 7459, – 2012. – PP. 541-556.
3. Can Xiang. Verifiable and Secure Outsourcing Schemes of Modular Exponentiations Using One Untrusted Cloud Server and Their Application // IACR Cryptology ePrint Archive 2014: PP.500 . – https://eprint.iacr.org/2014/500.pdf
4. Markovskyi O.P. Secure Modular Exponentiation in Cloud Systems. / Oleksandr P. Markovskyi, Nikolaos Bardis, Nikolaos Doukas, Sergej Kirilenko // Proceedings of The Congress on Information Technology, Computational and Experimental Physics (CITCEP 2015), 18-20 December 2015, Krakow, Poland, C. 266-269.