ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ И ПРОБЛЕМА БЕЗОПАСНОСТИ: АУТСОРСИНГ ВЫЧИСЛИТЕЛЬНО-СЛОЖНЫХ ЗАДАЧ С СЕКРЕТНЫМИ ДАННЫМИ

Е. Н. Сейткулов

Евразийский национальный университет имени Л. Н. Гумилева
Астана, Казахстан
E-mail: seitkulov_y@enu.kz

Проблема быстрых вычислений актуальна во всех сферах социально-экономического развития: быстрая обработка данных в облаке, безопасное хранение в облаке, быстрые вычисления сложно-вычислительных задач в облаке и т. д. В настоящее время имеет место бурное развитие аутсорсинговых услуг: различные IT-компании реализовывают услуги по хранению данных; другие же специализированные компании предлагают за определенную плату реализовывать сложно-вычислительные задачи (распределенные вычисления, grid-технологии). Данная работа посвящена разработкам методов безопасного аутсорсинга для целого класса как линейных, так и нелинейных уравнений.

Ключевые слова: безопасный аутсорсинг, безопасные облачные вычисления.

Современные технологии аутсорсинга вдохновлены многочисленными проблемами в области вычислительной математики, где решения рассматриваются в виде их приближений. Примеры таких задач могут быть найдены в области экономики, военной, нефтяной промышленности, а также в других областях. Многие из научных и численных проблем современности требуют больших вычислительных ресурсов, поэтому они могут быть решены только на суперкомпьютерах либо с использованием возможностей крупнейших вычислительных систем, таких как грид-технология, облако и т. д.

Необходимость аутсорсинга научных вычислений возникает в том случае, когда Клиенту нужно решить некую задачу, но он для этого не имеет соответствующих вычислительных мощностей. Эффективным выходом из данной ситуации является использование внешнего сервера для выполнения трудных вычислений. Такая форма аутсорсинга позволяет Клиентам с ограниченными ресурсами осуществлять трудоемкие вычисления в облаке и пользоваться большой вычислительной мощностью по сниженной стоимости. Но, несмотря на преимущества, проблемы безопасности часто становятся основным препятствием, которое ограничивает применение этой модели.

Основная идея, позволяющая обеспечить определенный уровень секретности для Клиента, это выполнение тщательной предварительной обработки задачи, прежде чем отправить ее на сервер, а также некоторые пост-процессорные операции полученных результатов от сервера, чтобы извлечь правильный ответ.

Способы безопасного научного аутсорсинга (умножения матриц, решения дифференциальных уравнений, задачи линейного программирования и т. д.) были обсуждены в публикациях [1–10]. Большинство из этих способов основаны на математических методах обработки (маскировки) со стороны Клиента. Многие технологии обработки научных вычислений предложены в [9]. Следует также отметить, что проблема ускорения безопасных вычислений с использованием вспомогательного

(внешнего) компьютера впервые была озвучена в качестве предмета теории информационной безопасности в [10]. Идея использования вспомогательных компьютеров для решения задач с секретными параметрами – предмет исследований, проведенных многими криптографами. Очень много результатов было получено для решения задач с использованием криптосистемы RSA. В работах Е. Н. Сейткулова [11–13] предложены методы безопасного аутсорсинга научных вычислений, однако методы исследователя радикально отличаются в том смысле, что некоторые части задачи остаются известны всем, включая злоумышленников. Такой подход делает обеспечение безопасности более сложным. Новизна в работах Е. Н. Сейткулова – использование внутренних свойств уравнений, например для решения линейного дифференциального уравнения с секретными параметрами используются свойства фундаментальной системы решений.

Целью исследования является представление различных методов нахождения приближенных решений уравнений с секретными параметрами с помощью внешнего компьютера. Для этого мы выбрали некоторые классы алгебраических и дифференциальных уравнений, так как в большинстве случаев современные вычислительные задачи сводятся к решению таких систем уравнений (дифференциальных уравнений, линейное программирование и т. д.). Исследование опирается на методы (линеаризация, методы сдвига), разработанные Е. Н. Сейткуловым для задач безопасного научного аутсорсинга.

Результаты исследования опубликованы в журнале с ненулевым импакт-фактором [11]. В опубликованной работе представлен ряд методов безопасного аутсорсинга научных вычислений. Рассмотрены протоколы решения абстрактных уравнений с секретными параметрами вида $Ax = f$. Такие уравнения изучались также другими исследователями, например [9], но представленные нами методы радикально отличаются от полученных ранее.

На конференции будут приведены основные подходы для решения линейных уравнений с секретными параметрами. Новым подходом в данной области исследования является использование внутренних свойств линейных дифференциальных уравнений, таких как свойства фундаментальной системы решений. Представленные методы существенно используют линейность рассматриваемых уравнений.

Далее будут представлены методы решения нелинейных уравнений с использованием результатов теории аналитических функций, что также является новизной в области безопасного аутсорсинга. Будет рассмотрена прикладная задача построения карты распределения полезных ископаемых в заданной области с секретными пробными данными. Необходимость изучения данного вопроса связана с тем, что обработка огромного массива данных, полученных в результате геологоразведовательных исследований, возможна только с использованием мощностей суперкомпьютерных технологий. Поэтому и возникает проблема безопасного аутсорсинга для задач подобного рода. В данной задаче секретными данными являются результаты геологоразведовательных исследований, т. е. пробные данные в различных точках области обнаружения полезных ископаемых.

Библиографические ссылки

1. *Atallah M., Frikken K.* Securely outsourcing linear algebra computations // in Proc. of ASIACCS. 2010. P. 48–59.

2. *Gennaro R., Gentry C., Parno B.* Non-interactive verifiable computing: Outsourcing computation to untrusted workers // in Proc. Of CRYPTO'10. Aug. 2010.
3. Secure ranked keyword search over encrypted cloud data / C. Wang [et all] // in Proc. of ICDCS'10. 2010.
4. *Yu S., Wang C., Ren K., Lou W.* Achieving secure, scalable, and fine-grained access control in cloud computing // in Proc. of IEEE INFOCOM'10, San Diego, CA, USA. March. 2010.
5. *Benjamin D., Atallah M. J.* Private and cheating-free outsourcing of algebraic computations // in Proc. of 6th Conf. on Privacy, Security, and Trust (PST). 2008. P. 240–245.
6. *Akimanaa R., Markowitch O., Roggeman Y.* Grids confidential outsourcing of string matching // The 6th WSEAS Int. Conf. on Software Engineering, Parallel and Distributed Systems, 2007.
7. *Atallah M. J., Li J.* Secure outsourcing of sequence comparisons // Int. J. Inf. Sec., 2005. V. 4. № 4, P. 277–287.
8. *Hohenberger S., Lysyanskaya A.* How to securely outsource cryptographic // Proc. of TCC. 2005. P. 264–282.
9. *Atallah M. J., Pantazopoulos K. N., Rice J. R., Spafford E. H.* Secure outsourcing of scientific computations, Advances in Computers, 2001. V. 54. P. 216–272.
10. *Matsumoto S., Kato K., Imai H.* Speeding up secret computations with insecure auxiliary devices // Proceedings on advances in Cryptology – Crypto '88, LNCS 403, Springer-Verlag. P. 497–506. 1990.
11. *Seitkulov Ye.* New methods of secure outsourcing of scientific computations // The Journal of Supercomputing, 2012, Springer US, V.62, P. 1–16. ISSN 0920-8542 (Print) 1573-0484 (Online).
12. *Seitkulov Ye., Otelbaev M.* Cloud computing technology: secure outsourcing of scientific computations // Сб. тр. междунар. конф. «Функциональный анализ и его приложения», октябрь 2012. С. 302–303.
13. *Сейткуло, Е. Н., Ергалиева Б. Б.* Один метод хранения информации в облаке в зашифрованном виде с использованием технологии разделения секрета // Сб. тр. междунар. конф. «Функциональный анализ и его приложения», октябрь 2012. С. 283–284.