УДК 004.021

АНАЛИЗ ОТКАЗОУСТОЙЧИВОСТИ АЛГОРИТМОВ ГОМОМОРФНОГО ШИФРОВАНИЯ ПРИ ОРГАНИЗАЦИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Вавилова А.С.
alina.vavilova.96@rambler.ru, 89992122317
(Университет ИТМО)
Научный руководитель – к.т.н., доцент Левина А.Б.
(Университет ИТМО)

Обеспечение конфиденциальности передаваемых данных в условиях растущих вычислительных мощностей устройств злоумышленников и появлению новых способов деструктивного воздействия на работу систем удаленной обработки информации является ключевой проблемой при организации различных облачных сервисов. Алгоритмы гомоморфного шифрования позволяют производить операции над зашифрованными данными без предварительного дешифрования, что значительно снижает риск рассекречивания конфиденциальной информации при удаленной обработке. Одной из главных задач при организации облачных вычислений с применением полностью гомоморфных алгоритмов шифрования является обеспечение непрерывности функционирования таких систем при осуществлении попыток взлома. В представленной работе проведен анализ отказоустойчивости алгоритмов гомоморфного шифрования и разработаны рекомендации по уменьшению вероятности возникновения ошибки при работе систем удаленной обработки данных.

В настоящее время во многих сферах деятельности человека наблюдается потребность в удаленной обработке информации, например, для организации генных банков, при обработке больших данных систем управления технологическими процессами или для осуществления удаленных тестирований уровня знаний в рамках реализации образовательных программ. Существующие решения различных облачных сервисов основаны на передаче информации от потребителя к серверам обработки данных по открытым каналам связи и предполагают обработку информации в незашифрованным виде, что требует дополнительных мер по обеспечению конфиденциальности входных данных и результатов работы систем облачных вычислений. Внедрение алгоритмов гомоморфного шифрования в протоколы обмена информацией и использование гомоморфно соответствующих функций в процессе получения результатов облачных вычислений позволяют достигнуть более высокого уровня обеспечения безопасности во время передачи, обработки и хранения данных. Для повышения производительности облачных систем обработки информации возможны аппаратные реализации алгоритмов гомоморфного шифрования, появление которых может привезти к возникновению множественных сбоев и программных ошибок в связи с многомодульностью подобных решений. Проведение анализа отказоустойчивости алгоритмов гомомофрного шифрования является необходимым этапов в процессе обеспечения непрерывности функционирования облачных систем.

При построении высоконагруженных систем управления технологическими процессами важно учитывать множество пользователей – источников входных данных. Облачная система является отказоустойчивой в случае корректной обработки информации при отказе отдельных её элементов, неполноте полученных данных (например, компрометации одного из источников данных или отсутствие одного из поступающих на обработку параметров) и возникновения ненулевого значения переменной накопления ошибки.

Для проведения анализа отказоустойчивости рассматривается каждый вычислительный модуль алгоритма гомоморфного шифрования и соответствующие наборы входных и выходных данных.

В качестве механизма для уменьшения вероятности возникновения ошибки при работе систем удаленной обработки данных рассматривается возможность внедрения дополнительного модуля поиска случайных ошибок в вычислительных модулях гомоморфно соответствующих операций с входными данными и зашифрованными значениями, хранящихся в памяти облачной системы. Предлагаемый способ упростит выявление кластерных многоразрядных сбоев, незначительно увеличив время работы системы, и уменьшит размер занимаемого объема памяти для хранения переменных системы.

На основе проведенного анализа отказоустойчивости алгоритмов гомоморфного шифрования при организации облачных вычислений разработаны рекомендации по уменьшению вероятности возникновения ошибки при работе систем удаленной обработки данных с расчетом целесообразности дополнительно затрачиваемых временных ресурсов в ходе выполнения одного цикла работы облачной системы и уменьшения необходимого объема памяти для хранения ресурсов системы.