УДК 621.396

Максимова София Михайловна

ПРИМЕНЕНИЕ ГОМОМОРФНОГО ШИФРОВАНИЯ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

В статье рассматривается концепция гомоморфного шифрования как инновационной формы шифрования, позволяющей обрабатывать данные, не расшифровывая их заранее. Подчеркивается, что гомоморфное шифрование нахо-

дит широкое применение в облачных хранилищах и базах данных, обеспечивая высокий уровень конфиденциальности и безопасности. Объяснено различие типов гомоморфного шифрования, таких как частичное, ограниченное и полное, и выделена важность использования этих методов для защиты данных в различных сценариях, включая обслуживание облачных сервисов и электронное голосование. В статье указано на ограничения существующих алгоритмов гомоморфного шифрования и необходимость дальнейших исследований в этой области для обеспечения высокого уровня безопасности данных.

Гомоморфное шифрование, криптография, обработка данных, конфиденциальность, облачное хранилище, ограничения алгоритмов.

Maximova Sofia Mikhailovna

THE USE OF HOMOMORPHIC ENCRYPTION IN THE FIELD OF CYBERSECURITY

The article discusses the concept of homomorphic encryption as an innovative form of encryption that allows you to process data without decrypting it in advance. It is emphasized that homomorphic encryption is widely used in cloud storage and databases, providing a high level of confidentiality and security. The difference between the types of homomorphic encryption, such as partial, limited and complete, is explained, and the importance of using these methods to protect data in various scenarios, including cloud services and electronic voting, is highlighted. The article points out the limitations of existing homomorphic encryption algorithms and the need for further research in this area to ensure a high level of data security.

Homomorphic encryption, cryptography, data processing, privacy, cloud storage, algorithm limitations.

Введение

Гомоморфное шифрование (ГШ) – это революционная криптографическая технология, позволяющая выполнять вычисления над зашифрованными данными без необходимости их предварительной расшифровки. Данные шифруются с помощью специального алгоритма, создавая "зашифрованный контейнер", который скрывает информацию от посторонних глаз. Зашифрованные данные обрабатываются как обычные, но все операции происходят внутри "контейнера", не затрагивая исходную информацию. Результат вычислений, полученный в зашифрованном виде, расшифровывается, предоставляя достоверный ответ без раскрытия исходных

данных. В следствие этого данные остаются защищены на протяжении всего процесса обработки, даже на серверах поставщиков услуг [4].

Основная часть

Гомоморфное шифрование находит особое применение в сценариях, где данные хранятся и обрабатываются в облачных хранилищах или базах данных, поскольку оно гарантирует, что конфиденциальные данные остаются в безопасности, даже если они обрабатываются третьими лицами. Это представляет собой значительный прогресс в криптографии и предлагает мощный инструмент для защиты конфиденциальности данных. Традиционные методы требуют, чтобы данные были расшифрованы перед обработкой, в то время как гомоморфные алгоритмы позволяют оставаться им в зашифрованном виде на протяжении всей обработки [1]. Это можно сравнить с конвертом, который можно вскрыть, не раскрывая его содержимого, что обеспечивает безопасную обработку данных при сохранении их конфиденциальности.

Концепция гомоморфного шифрования была впервые представлена в 1978 году, что привело к разработке алгоритма RSA. Однако полностью гомоморфные системы были реализованы только в 2009 году [10].

Существует несколько типов гомоморфного шифрования, включая частичное, ограниченное и полное гомоморфное шифрование. Частичное гомоморфное шифрование допускает проведение неограниченного количества одинаковых операций, в то время как ограниченное гомоморфное шифрование допускает только определенное количество операций. Полное гомоморфное шифрование обеспечивает неограниченное разнообразие операций и является самым мощным из трех типов [6]. Полностью гомоморфная криптосистема позволяет оценивать любую схему, что означает возможность разработки программы для работы с зашифрованными входными данными, производя зашифрованные выходные данные. Эти программы не расшифровывают свои данные, что позволяет им выполняться третьими сторонами без раскрытия содержащейся информации или внутреннего состояния. Это позволяет передавать вычислительные задачи на аутсорсинг в облако [2].

Использование зашифрованных данных в вычислениях помогает решить различные проблемы безопасности. Хранение данных в облаке с использованием гомоморфного шифрования обеспечивает их безопасность и конфиденциальность [1]. Это устраняет необходимость делиться ключами дешифрования с неавторизованными пользователями, тем самым снижая

риск утечки данных. Это также избавляет от необходимости полагаться на поставщиков услуг для безопасной передачи данных, поскольку доступ к данным будут иметь только авторизованные пользователи.

Использование медицинских данных для машинного обучения не представляет никаких рисков для пациентов и не требует удаления личной информации, поскольку вся информация зашифрована с самого начала. Результаты обработки также зашифрованы, и получить к ним доступ можно только с помощью правильного ключа расшифровки, что предотвращает несанкционированный доступ.

Проведение профилирования клиентов во время передачи данных маркетинговым компаниям не нарушает конфиденциальность, пока клиенты сохраняют контроль над своим ключом к данным. В этом случае целевая реклама по-прежнему может быть настроена и является менее агрессивной, чем другие формы маркетинга. Гомоморфное шифрование устраняет необходимость в предварительной оценке мер защиты персональных данных при трансграничной передаче данных, поскольку такие требования устраняются, когда данные шифруются с использованием методов гомоморфного шифрования.

В облачных вычислениях гомоморфное шифрование показывает себя с лучшей стороны [2]. Гомоморфное шифрование обладает огромным потенциалом для повышения безопасности и конфиденциальности данных в облачных вычислениях. По мере развития технологий и снижения вычислительных затрат ГШ станет более доступным и широко используемым [9]. Данные защищены даже во время обработки в облаке, что снижает риски несанкционированного доступа и утечки информации, а анализ данных позволяет извлечь ценные сведения без ущерба для конфиденциальности. ГШ обеспечивает гибкость и масштабируемость при работе с конфиденциальными данными в облаке, позволяя легко добавлять новых пользователей и расширять объемы данных.

Одним из наиболее существенных преимуществ полностью гомоморфного шифрования является его способность выполнять математические операции с данными, хранящимися в удаленном облачном хранилище [3]. Этот тип шифрования позволяет защищенным облачным сервисам выполнять различные операции с пользовательскими данными без ущерба для конфиденциальности фактического содержимого.

Информационная безопасность в облачных вычислениях стала предметом обсуждения лишь недавно, после широкого внедрения облачных

сервисов. Однако опыт работы с этими сервисами показал, что существующих криптографических методов недостаточно для защиты данных в этой среде. Защита данных в облаке представляет собой более сложную задачу, чем могут решить традиционные методы, и в некоторых случаях систем открытых ключей может оказаться недостаточно для защиты конфиденциальной информации [5].

Как упоминалось ранее, ГШ позволяет хранить и обрабатывать конфиденциальные данные в облачных сервисах без необходимости их расшифровки на стороне сервера. Это обеспечивает более высокий уровень безопасности, чем традиционные методы шифрования, и снижает риски утечки информации [3][5]. Из-за важности производительности в облачных вычислениях крайне важно использовать различные алгоритмы, адаптированные к конкретным требованиям. Следует изучить альтернативные методы для операций сортировки и сравнения. Для создания полнофункциональной гомоморфной системы шифрования важно ограничить количество манипуляций, выполняемых с данными, сохраняя при этом критические пороговые значения допуска ошибок [2].

Гомоморфное шифрование может играть ценную роль в гибридных облачных средах, где конфиденциальные данные хранятся как в локальной инфраструктуре, так и в общедоступном облаке. Оно позволяет выполнять вычисления над зашифрованными данными, хранящимися в общедоступном облаке, без их предварительной расшифровки. Это обеспечивает конфиденциальность данных, даже когда они обрабатываются на серверах стороннего поставщика и помогает компаниям соответствовать строгим требованиям к конфиденциальности данных, таким как GDPR и HIPAA, при использовании гибридных облачных решений [3].

ГШ обладает потенциалом для революционного изменения системы электронного голосования. Шифрование позволяет избирателям кодировать свои голоса, гарантируя, что их выбор останется конфиденциальным и тем самым обеспечивает прозрачность процесса голосования, позволяя проводить аудит и проверку результатов без раскрытия личности избирателей. Это защищает голоса от фальсификации и манипулирования, делая систему электронного голосования более надежной.

Пример системы электронного голосования с применением гомоморфного шифрования выглядит следующим образом [4]:

1. Избиратели разделили бы свои голоса на несколько частей, используя секретный метод;

2. Представители подсчитают неполные голоса. Благодаря свойствам гомоморфного шифрования окончательный результат голосования будет сохранен в тайне;

3. Шифрование гарантирует, что выбор каждого избирателя останется конфиденциальным. Никто не может отследить, как человек проголосовал. Алгоритмы ГШ обеспечивают точный подсчет голосов, исключая возможность манипулирования или фальсификации, а система позволяет проводить аудит и проверку результатов без раскрытия личности избирателей. Использование гомоморфного шифрования может повысить доверие к системе электронного голосования, делая ее более прозрачной и подотчетной [1].

Электронное голосование с ГШ может быть более быстрым, удобным и экономичным, чем традиционные методы. Это может сделать голосование более доступным для людей с ограниченными возможностями и обеспечить более высокую безопасность от фальсификации и манипулирования голосами, чем бумажные бюллетеня [8].

Системы голосования должны быть спроектированы таким образом, чтобы предотвращать мошеннические действия, такие как многократное голосование, фальсификация результатов голосования и дублирование записей. Избирателям, имеющим право голоса, должно быть разрешено голосовать только с использованием электронной системы. Система электронного голосования, использующая гомоморфное шифрование, обеспечивает конфиденциальность каждого голоса. Голоса кодируются как 0 или 1, поэтому личность избирателя не может быть привязана к его бюллетеням. Результаты голосования регистрируются в публичном реестре, что позволяет любому желающему убедиться в том, что его голос был подсчитан [7]. В конце процесса голосования алгоритм подсчитывает общее количество голосов и шифрует его, используя конфиденциальный код, известный только группе назначенных лиц, которые обеспечивают точность и конфиденциальность результатов. Этот процесс помогает сохранить целостность системы голосования, предотвращая мошеннические действия и защищая частную жизнь избирателей [6]. Существенной проблемой в системах электронного голосования является обеспечение точной регистрации и защита результатов голосования от изменения. Это достигается за счет использования методов гомоморфного шифрования, которые позволяют проверять зашифрованные голоса, не раскрывая фактического выбора.

Эти методы основаны на доказательствах с нулевым разглашением, которые гарантируют, что голосование может иметь только два возможных результата, и требуют проверки избирателя для подтверждения бюллетеня [1]. Процесс голосования проводится с использованием нескольких сетей, чтобы предотвратить вмешательство сторон, не имеющих полномочий, в результаты. Для защиты процесса и обеспечения анонимности и конфиденциальности каждого голосования используются передовые методы шифрования. После того, как голоса были зашифрованы, их можно расшифровать, но их нельзя привязать к конкретным избирателям без помощи доверенного лица, имеющего доступ к ключу дешифрования. Как только бюллетени будут проверены на точность (0 или 1), их можно будет сравнить с критериями, указанными в процессе голосования. Однако убедиться в том, что избиратели не потеряли или не изменили свои бюллетени и что за них не были поданы дополнительные голоса, может быть непросто. Для решения этой проблемы, возможно, потребуется принять дополнительные меры проверки.

Выводы

Поскольку технологии криптографии и кибербезопасности продолжают развиваться, гомоморфное шифрование становится все более перспективной областью исследований. Несмотря на все ограничения, ГШ обладает огромным потенциалом для изменения подхода к безопасности и конфиденциальности данных в различных областях. Ожидается, что ГШ будет играть все более важную роль в областях защиты данных в здравоохранении, финансовых и государственных услугах.

В ближайшем будущем подобные виды шифрования, вероятно, окажут значительное влияние на рынок криптографических услуг. По мере развития технологий и снижения вычислительных затрат они станут более доступны и широко используемы.

Хотя частично гомоморфные схемы применяются для сложения и умножения в таких областях, как облачные вычисления и системы электронного голосования, они полезны только в определенных сценариях [1][4]. Эти схемы позволяют выполнять определенные операции без расшифровки данных, обеспечивая определенный уровень безопасности. Однако важно отметить, что они не всегда обеспечивают полную защиту и могут быть подвержены атакам. Поэтому некоторые гомоморфные методы могут подходить не для всех случаев передачи данных, требующих высокого уровня защиты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Поляков А.С.* Анализ возможностей алгоритмов международного стандарта «Облегченная криптография» – ISO/IEC 29192-2:2012 / А.С. Поляков, В.Е. Самсонов // Информатика. – 2014. – № 3. – С. 107–112.

2. *Батура Т.В.* Облачные технологии: основные понятия, задачи и тенденции развития / Т.В. Батура Ф.А. Мурзин, Д.Ф. Семич // Программные продукты и системы. – 2014. – № 3. – С. 64–72.

3. *Афанасьев С.В.* Облачные сервисы, онтологическое моделирование таксономии / С.В. Афанасьев // Труды СПИИРАН. – 2012. – № 23. – С. 392–399.

4. *Варновский Н.П.* Гомоморфное шифрование / Н.П. Варновский, А.В Шокуров // Труды Ин-та системного программирования РАН. – 2006. – Т. 12. – С. 27–36.

5. *Жиров А.О.* Безопасные облачные вычисления с помощью гомоморфной криптографии / А.О. Жиров, О.В. Жирова, С.Ф. Кренделев // Безопасность информационных технологий. – 2013. – Т.1. – С. 6–12.

6. Batch fully homomorphic encryption over the integers / J.H. Cheon [et al.] // Advances in Cryptology – EUROCRYPT'2013 (LNCS). – 2013. – Vol. 7881. – P. 315–335

7. *Заргарян Е.В., Морозов Н.В.* Необходимость разработки системы обнаружения утечек на нефтепроводе/ В сборнике: Донецкие чтения 2023: образование, наука, инновации, культура и вызовы современности. Материалы VIII Международной научной конференции. Донецк, 2023. С. 141-143.

8. *Заргарян Е.В., Рой Ю.В.* Сепарация газа на промыслах и типы применяемых устройств. В сборнике: Технологии разработки информационных систем ТРИС-2020. Материалы X Международной научно-технической конференции. "Технологии разработки информационных систем", 2020. С. 143-149

9. *Ганциевский А.В., Заргарян Е.В.* Анализ существующих методов оптической сепарации ТБО/ Молодёжный вестник Новороссийского филиала Белгородского государственного технологического университета им. В.Г. Шухова. 2023. Т.3. №2 (10). С. 188-191.

10. *Заргарян Е.В., Филонова Е.С.* Эффекты применения технологий IIOT в системах интеллектуального управления освещением на производстве// В сборнике: Прикладные вопросы точных наук. Материалы VII Международной научно – практической конференции студентов, аспирантов, преподавателей. 2023. С. 121 – 124.

Максимова София Михайловна, студентка Политехнического института (филиал) ДГТУ в г. Таганроге, Россия, город Таганрог, улица Петровская 109а, 347904, телефон: +7 (928) 778-71-94, email: sofiamaksimova.2003@mail.ru.

Maximova Sofia Mikhailovna, student of the Polytechnic Institute (branch) of DSTU in Taganrog, Russia, Taganrog, Petrovskaya street 109a, 347904, phone: +7 (928) 778-71-94, email: sofiamaksimova.2003@mail.ru.