УДК 004.056.53

С.А. Быстревский, А.Е. Боршевников, Ю.В. Добржинский

Протокол верификации данных для схемы конфиденциальных вычислений с гомоморфным шифрованием

Большую роль в рамках современного общества получили системы аукционных торгов и технологии BigData. Однако за счет того, что обозначенные технологии могут работать с финансами их участников, возникает необходимость внедрения в них систем безопасности, обеспечивающих возможность верификации данных. Предложен протокол верификации данных на основе применения гомоморфного шифрования. Показана формальная оценка безопасности разработанного протокола, а также проведён анализ с вероятностной точки зрения.
Ключевые слова: конфиденциальные вычисления, гомоморфное шифрование, верификация данных, аукционные торги.
DOI: 10.21293/1818-0442-2024-27-2-31-36

Одной из научно-исследовательских задач, которую стоит выделить в современном мире, является задача математически доказанного обезличивания информации для баз данных и систем, использующих технологии BigData [1]. Также следует выделить задачу обеспечения суверенитета экономических систем, устанавливаемую Указом Президента Российской Федерации от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации». Эти задачи порождают создание новых криптографических протоколов, которые будут обеспечивать конфиденциальность операций, в том числе конфиденциальных вычислений [2].

В настоящий момент можно выделить два подхода к построению протоколов конфиденциальных вычислений [3]:

1. На основе искажения логического контура. Данный подход эффективен для двух пользователей и, как правило, позволяет реализовывать функции сравнений, что не применимо для аукционных торгов, совместного расчёта по контрактам и другим специфическим видам аукционов [4, 5].
2. На основе схем разделения секрета. Данный подход эффективен для большого количества пользователей и, как правило, реализует арифметические функции. Однако данный подход сильно зависим от честности арбитра, участвующего в рамках протокола [6–9].

Таким образом, на данный момент нет эффективного подхода реализации алгоритмов конфиденциальных вычислений, подходящего под все виды экономических взаимодействий.

На основе вышесказанного планируется выделить новый подход, который позволит арбитру выступать в качестве посредника и устранит его влияние на систему, а также позволит реализовывать функции сравнения для большого количества пользователей. К примеру, подобные алгоритмы можно будет реализовывать в аукционных торгах с закрытыми ставками, в которых ставки не разглашаются и обозначается только победитель. Реализация такого протокола представлена в работе [2]. Цель данной статьи – представить общую схему для реализации протоколов верификации, используемую в алгоритмах конфиденциальных вычислений, на основе гомоморфных отображений. Также составление общей схемы позволит выделить общие плюсы и уязвимости данных подходов.

Конфиденциальные вычисления в задаче аукционных торгов

В настоящее время в задаче обеспечения конфиденциальности вычислений при проведении аукционных торгов можно выделить ряд различных решений.

Например, одним из решений, которое может использоваться в рамках данной задачи, является применение протокола блокчейн, обеспечивающего анонимизацию всех транзакций [10–12]. Дальнейшее развитие идея применения протокола блокчейн для решения проблемы конфиденциальных вычислений получила в работе [13], где совместно с блокчейн-технологией применялась схема доказательства знания с нулевым разглашением для проверки корректности полученного результата конфиденциальных вычислений. Недостатком указанных протоколов является высокая вычислительная сложность, необходимая для их выполнения. В работах [14, 15] был предложен алгоритм конфиденциальных вычислений с использованием гомоморфного шифрования для решения задачи проведения безопасных аукционных торгов. Однако указанные протоколы также не обеспечивают конфиденциальность вычислений в полной мере за счет трудоемкости выполнения операций, заложенных в их основу [16, 17].

Возможное применение алгоритма конфиденциальных вычислений с использованием гомоморфного шифрования в задаче аукционных торгов было показано в работе [2], однако в рамках предложенного протокола актуальным остается вопрос верификации данных, передаваемых пользователем, что требует разработки отдельных протоколов. В дальнейшем будет предложен один из возможных вариантов протокола верификации данных.

Гомоморфное шифрование

Необходимо ввести понятие гомоморфизма. Пусть даны две группы: **X** с определённой на ней

бинарной алгебраической операцией «*» и **Y** с операцией «×». Отображение G: $\mathbf{X}\to\mathbf{Y}$ между этими группами, которое каждому элементу множества **X** ставит в соответствие элемент из множества **Y**, будет называться гомоморфизмом, если будет выполняться следующее условие (1):

$$G(x_1 * x_2) = G(x_1) \times G(x_2), \forall x_1, x_2 \in \mathbf{X}. \quad (1)$$

Гомоморфное шифрование можно определить следующим образом. Пусть k – ключ зашифрования, m – исходное сообщение. Алгоритм шифрования E называется гомоморфным относительно операции «*», если существует полиномиальный алгоритм A, позволяющий вычислить для любых двух закрытых текстов $E_k(m_1)$, $E_k(m_2)$ значение $C = E_k(m_1*m_2) = A(E_k(m_1), E_k(m_2))$. При этом необходимо, чтобы по известным значениям C, $E_k(m_1)$, $E_k(m_2)$, но неизвестном значении ключа k, было невозможно эффективно проверить, что шифртекст C получен из шифртекстов $E_k(m_1)$ и $E_k(m_2)$.

На практике чаще рассматривается частный случай, где вместо полиномиального алгоритма A вводится операция на множестве шифртекстов «×», так, чтобы для любых двух закрытых текстов $E_k(m_1)$, $E_k(m_2)$ значение $C = E_k(m_1*m_2) = E_k(m_1)\times E_k(m_2)$. То есть существует некоторая операция на множестве закрытых текстов «×», которая равносильна операции на множестве открытых текстов «*».

Гомоморфная функция

Стоит определить алгоритм конфиденциальных вычислений, позволяющий доказать, что секрет принадлежит некоторому множеству значений, при этом не раскрывая значение секрета. Без потери общности можно считать, что в алгоритме конфиденциальных вычислений участвуют один пользователь P, имеющий секретное значение x, и арбитр A, который проверяет принадлежность значения x к заданному множеству **X**. Другими словами, подобную модель можно описать следующей функцией (2):

$$F(x) = \begin{cases} 1, & x \in \mathbf{X}; \\ 0, & x \notin \mathbf{X}. \end{cases} \quad (2)$$

Пользователь и арбитр применяют гомоморфное преобразование $E(m) = c$ с требованием, что функция E является односторонней (3):

$$E_k(m_1) \times E_k(m_2) = E_k(m_1 * m_2), \quad (3)$$

где × – операция взаимодействия с открытыми значениями, * – операция взаимодействия с закрытыми текстами.

Также арбитр и пользователи должны выбрать два множества значений **W** и **Y** так, чтобы выполнялись следующие свойства (4):

$$\mathbf{W}, \mathbf{Y}: \begin{cases} x * w \in \mathbf{Y}, \ \exists w \in \mathbf{W}, \ x \in \mathbf{X}; \\ x * w \notin \mathbf{Y}, \ \forall w \in \mathbf{W}, \ x \notin \mathbf{X}. \end{cases} \quad (4)$$

Протокол верификации

Формально протокол верификации можно определить следующим образом:

Вход: пользователь P с секретными значением x; арбитр A.

Выход: $F(x) = t: \ t = \begin{cases} 1, & x \in \mathbf{X}; \\ 0, & x \notin \mathbf{X}. \end{cases}$

1. $P \to A: \quad c = E(x); \quad w' = E(w): \ w \in \mathbf{W}, \ y = x * w \in \mathbf{Y}.$

2. $A \to P: \ b: \ b \in \{0, 1\}$ – случайный бит.

3. Если $b = 0$:

3.1. $P \to A: \ w.$

3.2. $A: \ t = \begin{cases} 1, & w' = E(w) \text{ и } w \in \mathbf{W}; \\ 0, & w' \neq E(w) \text{ и } w \in \mathbf{W}. \end{cases}$

4. Если $b = 1$:

4.1. $P \to A: \ y = x * w.$

4.2. $A: \ t = \begin{cases} 1, & w' \times c = E(y) \text{ и } y \in \mathbf{Y}; \\ 0, & w' \times c \neq E(y) \text{ и } y \in \mathbf{Y}. \end{cases}$

Выход: t.

Конец протокола.

В виде схемы данный протокол представлен на рис. 1.

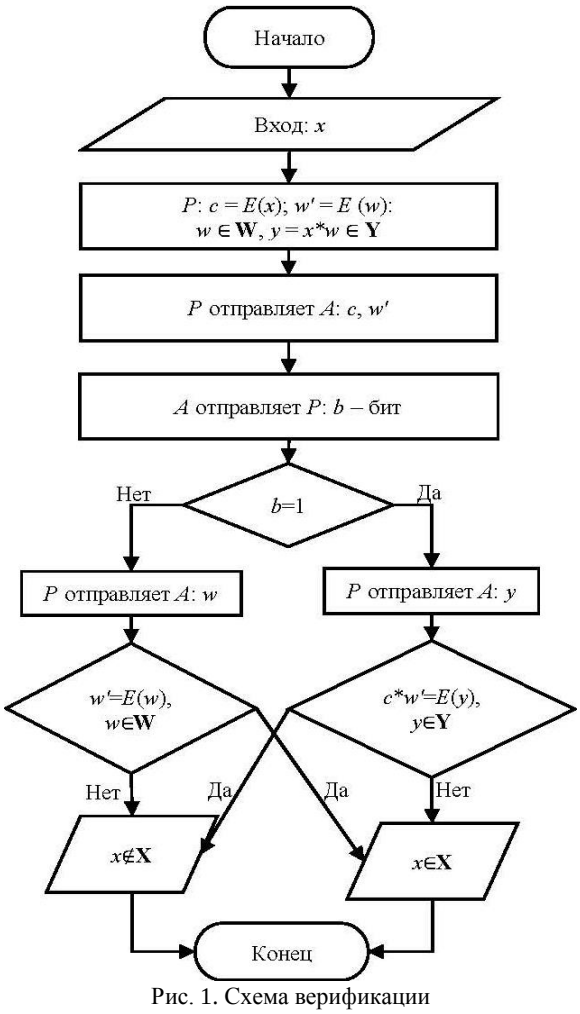

Рис. 1. Схема верификации

Указанный алгоритм построен по принципу «пещеры Али-Бабы», т.е. верифицируемый пользователь генерирует некоторые значения, после проверяющий требует подтвердить или правильность сгенерированных данных, или правильность секрета.

Причём выполнить оба требования невозможно, таким образом, алгоритм подтверждает правильность секрета с вероятностью 1/2 и однозначно определяет неправильность данных. Таким образом, данный алгоритм необходимо повторить n раз так, чтобы вероятность пройти протокол, не обладая верным секретом, была $1/2^n$. Для достаточно больших n вероятность пройти протокол будет крайне мала.

Доказательство корректности

Стоит показать, что если у пользователя $x \in \mathbf{X}$, то он сможет пройти оба требования арбитра. Так как $x \in \mathbf{X}$, то все значения на 1 шаге можно сгенерировать, исходя из условий множеств, заданных выше. Тогда в случае $b = 0$ арбитр просто проверит правильность значения w с помощью гомоморфного преобразования E. Так как это односторонняя функция, то и значения должны получиться одинаковые. В случае $b = 1$ арбитр проверит правильность данных, используя свойство гомоморфизма функции E.

Далее следует установить, что пользователь, у которого $x \notin \mathbf{X}$, не сможет выполнить оба требования одновременно. Исходя из условий выбора множеств, на 1-м шаге можно выполнить или $w \in \mathbf{W}$, или $x*w \in \mathbf{Y}$. Так как для выполнения обоих свойств придётся найти коллизию преобразования E, тогда арбитр разоблачит пользователя или при $b = 0$, если $x*w \in \mathbf{Y}$, или при $b = 1$, если $w \in \mathbf{W}$.

Доказательство безопасности

Необходимо проанализировать криптографическую безопасность предложенного алгоритма. В случае $b = 0$ арбитру или злоумышленнику достаётся только значение w, которое не даёт однозначного ответа о том, какое значение x у пользователя. В случае $b = 1$ арбитр получает $x*w$, но без знания w нельзя однозначно вычислить x, а значение w арбитр получает, только если бы выбрал $b = 0$. Таким образом, данный алгоритм не даёт однозначного ответа о значении пользователя.

Стоит отметить, что в данном случае гарантия получения данных обеспечивается гомоморфными свойствами и открытостью работы с данными. Также выполняется свойство невозможности проведения вычислений с секретом пользователя без ведома пользователя, так как протокол интерактивный.

Вероятностная оценка безопасности

Несмотря на то, что нельзя точно получить значение секрета в ходе протокола, всё же есть возможность оценить вероятность использования того или иного секретного значения.

Пусть $P(x_i)$ – это вероятность того, что у пользователя значение $x_i \in \mathbf{X}$. Если в начале протокола злоумышленник не обладает никакой информацией о значении секрета x, то в начале протокола $P(x_i) = \frac{1}{|\mathbf{X}|}$, где $|\mathbf{X}|$ – это количество элементов множества $\mathbf{X}$.

Пусть $P(w/x_i)$ – это вероятность, что пользователь выберет значение $w \in \mathbf{W}$, при условии, что у него значение $x_i \in \mathbf{X}$. Подмножество w_j подходящих значений для данного x_i – $\mathbf{W}_{x_i} = \{w: w \in \mathbf{W}, x_i * w \in \mathbf{Y}\}$.

В таком случае вероятность $P(w/x_i) = \frac{1}{|\mathbf{W}_{x_i}|}$, где $|\mathbf{W}_{x_i}|$ – это количество элементов множества $\mathbf{W}_{x_i}$.

Перед злоумышленником стоит задача посчитать $P(x_i/w)$, если арбитр отправил $b = 0$, т.е. найти вероятность значения пользователя x_i при условии, что он использовал w. И найти вероятность $P(x_i/y)$, если арбитр отправил $b = 1$. Другими словами, вероятность секрета пользователя x_i при условии, что он получил значение y. По сути, эти задачи схожи, так как $P(x_i/y) = P(x_i/w)$, где $w = y * x_i^{-1}$, т.е. все сходит к вопросу оценки вероятности $P(x_i/w)$. Таким образом, злоумышленник получит новое распределение вероятности секретного значения пользователя, что ослабляет безопасность протокола, но не делает его полностью уязвимым.

Вероятность $P(x_i/w)$ можно оценить с помощью теоремы Байеса (5):

$$P(x_i / w) = \frac{P(w / x_i)}{P(w)} = \frac{P(x_i) \cdot P(w / x_i)}{\sum_{j=1}^{|\mathbf{X}|} P(x_j) \cdot P(w / x_j)} = \frac{P(x_i) \cdot |\mathbf{W}_{x_i}|}{\sum_{j=1}^{|\mathbf{X}|} P(x_j) \cdot |\mathbf{W}_{x_j}|}. \quad (5)$$

В чистом виде данную вероятность найти трудно, но это и не требуется, так как общий интерес представляет, как изменится распределение вероятностей. Для этого стоит рассчитать отношение вероятностей (6):

$$\frac{P(x_i / w)}{P(x_j / w)} = \frac{P(x_i) \cdot P(w / x_i)}{P(w)} \times \frac{P(w)}{P(x_j) \cdot P(w / x_j)} = \frac{P(x_i) \cdot P(w / x_i)}{P(x_j) \cdot P(w / x_j)} = \frac{P(x_i) \cdot |\mathbf{W}_{x_i}|}{P(x_j) \cdot |\mathbf{W}_{x_j}|}. \quad (6)$$

То есть отношение вероятностей $P(x_i)/P(x_j)$ изменяется в зависимости от отношения $|\mathbf{W}_{x_i}|/|\mathbf{W}_{x_j}|$. В случае если мощность какого-то из множеств равно 0, то вероятность обнулится и отношение находить не имеет смысла. Таким образом, можно сделать вывод: чтобы система оставалась стабильной, необходимо, чтобы отношение $|\mathbf{W}_{x_i}|/|\mathbf{W}_{x_j}| = 1$ или хотя бы не сильно отличалось. В данном случае злоумышленник не сможет изменить отношение вероятностей. К сожалению, на практике такого добиться трудно, и необходимо максимально уменьшить отношение мощностей множеств.

Также важно отметить, что если неправильно выбрать множества $\mathbf{W}$ и $\mathbf{Y}$, то может возникать ситу-

ация, когда $P(x_i/w) = 0$. В таком случае злоумышленник полностью отбрасывает данный вариант секрета, а вероятность $P(x_i)$ распределяется между вероятностями остальных секретных значений. Отсюда самый оптимальный вариант, при котором не будет меняться распределение вероятностей, – это вариант, при котором условие (4) будет принимать следующий вид (7):

$$\mathbf{W},\ \mathbf{Y}: \begin{cases} x^* w \in \mathbf{Y}, & \forall w \in \mathbf{W}, \quad x \in \mathbf{X}; \\ x^* w \notin \mathbf{Y}, & \forall w \in \mathbf{W}, \quad x \notin \mathbf{X}. \end{cases} \qquad (7)$$

Для данного случая значения секрета отбрасываться не будут и не будет смещаться распределение вероятностей. На практике, как правило, такое не всегда выходит, так что при выборе множеств необходимо учитывать вероятностную оценку протокола, зависящую от выбора множеств **W** и **Y**.

Оценка сложности

Сложность описанного протокола можно оценить следующим образом. Так как количество итераций и вычислений в данном протоколе строго устанавливается, то сложность такого алгоритма зависит от сложности самих вычислений, т.е. сложность полиномиальная, так как вычисления должны удовлетворять такому свойству, иначе нет смысла использовать их в протоколе. В целом можно сказать, что сложность предложенного протокола будет сопоставима со сложностью гомоморфного преобразования E.

Заключение

В итоге стоит отметить, что данный протокол удовлетворяет требованиям безопасности, а гомоморфное шифрование не даёт возможности арбитру нарушить порядок вычислений, т.е. даёт гарантию получения информации. Система не имеет детерминированного алгоритма получения секрета. Однако данная система уязвима к вероятностной оценке распределения секретных значений пользователя. Таким образом, необходимо или минимизировать количество итераций алгоритма, или минимизировать отношение мощностей множеств $\left|\mathbf{W}_{x_i}\right| / \left|\mathbf{W}_{x_j}\right|$.

Предложенный алгоритм верификации способен определить принадлежность секрета к некоторому множеству. Для более точной оценки безопасности и эффективности протокола можно выделить следующие направления исследований:

– рассмотрение алгоритмов гомоморфного шифрования для применения в алгоритме;

– проверка корректности требований безопасности и эффективности для больших данных.

Данный протокол выделяет принципиально новый подход к разработке алгоритмов верификации и показывает, что он может устранить недостатки старых подходов и решать проблемы, которые ранее нельзя было решить.

Общая схема позволит формально оценить протоколы верификации, построенные по такому типу. Вариация такого протокола использовалась в работе [2]. Также данная схема позволит реализовывать другие протоколы конфиденциальных вычислений.

Исследование проведено при финансовой поддержке Минобрнауки России («Грант ИБ МТУСИ») № 40469-08/23-К.

Литература

1. Технологии доверенного взаимодействия в экосистеме Национальной технологической инициативы / А.А. Шелупанов, Д.С. Брагин, А.А. Конев, Р.А. Пермяков // Современное образование: интеграция образования, науки, бизнеса и власти: матер. междунар. науч.-метод. конф. – Томск: Изд-во ТУСУР, 2022. – Ч. 2. – С. 15–20.

2. Быстревский С.А. Об одном алгоритме конфиденциальных вычислений на основе гомоморфного шифрования для проведения аукционных торгов / С.А. Быстревский, А.Е. Боршевников // Молодежь. Наука. Инновации: сб. докл. 65-й Междунар. молодежной науч.-техн. конф. – Владивосток: Мор. гос. ун-т., 2023. – Т. 1. – С. 143–148.

3. Загартдинов Б.Н. Анализ реализации технологий конфиденциальных вычислений / Б.Н. Загартдинов, М.В. Поляков // Вопросы кибербезопасности. – 2023. – № 6 (58). – С. 122–127.

4. Берешполов И.С. Алгоритм кластеризации данных для защиты конфиденциальной информации в сети Интернет / И.С. Берешполов, Ю.А. Кравченко, А.Г. Слепцов // Известия ЮФУ. Технические науки. – 2023. – № 3 (233). – С. 74–85.

5. Schneider T. GMW vs. Yao? Ecient Secure Two-Party Computation with Low Depth Circuits / Thomas Schneider, Michael Zohner // ACS Sensors. – 2017. – Vol. 2, No. 8. – P. 1128–1132.

6. Запечников С.В. Конфиденциальное машинное обучение на основе двусторонних протоколов безопасных вычислений / С.В. Запечников, А.Ю. Щербаков // Безопасность информационных технологий. – 2021. – Т. 28, № 4. – С. 39–51.

7. Запечников С.В. Конфиденциальное машинное обучение на основе трехсторонних протоколов безопасных вычислений // Безопасность информационных технологий. – 2022. – Т. 29, № 1. – С. 30–43.

8. Запечников С.В. Конфиденциальное машинное обучение на основе четырехсторонних протоколов безопасных вычислений // Безопасность информационных технологий. – 2022. – Т. 29, № 2. – С. 46–56.

9. Asharovy G. A Full Proof of the BGW Protocol for Perfectly Secure Multiparty Computation / G. Asharovy, Y. Lindelly // DSPA: Issues of application of digital signal processing. – 2018. – Vol. 8, No. 1. – P. 12–17. DOI: 10.1007/s00145-015-9214-4.

10. Airtnt: Fair exchange payment for outsourced secure enclave computations / M. Al-Bassam, A. Sonnino, M. Krol, I. Psaras // arXiv preprint arXiv:1805.06411. – 2018. – URL: https://arxiv.org/pdf/1805.06411, свободный (дата обращения: 23.07.2024).

11. Tesseract: Real-time cryptocurrency exchange using trusted hardware / I. Bentov, Y. Ji, F. Zhang, Y. Li, X. Zhao, L. Breidenbach, P. Daian, A. Juels // Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. – 2019. – P. 1521–1538. DOI: 10.1145/3319535.3363221.

12. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts / R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, D. Song // 2019 IEEE European Symposium on Security and Privacy (EuroS&P). – 2019. – P. 185–200. DOI: 10.1109/EuroSP.2019.00023.

13. Galal H.S. Succinctly verifiable sealed-bid auction smart contract / H.S. Galal, A.M. Youssef // Data Privacy

Mana-gement, Cryptocurrencies and Blockchain Technology. – Springer, 2018. – P. 3–19. DOI: 10.1007/978-3-030-00305-0_1.

14. Казарин О.В. Разработка методов проактивной защиты информационных систем на основе конфиденциальных вычислений // Вопросы защиты информации. – 2013. – № 3 (102). – С. 68–80.

15. Пороговые схемы гомоморфного шифрования и защита информации в облачных вычислениях / Н.П. Варановский, С.А. Мартишин, М.В. Храпченко, А.В. Шокуров // Вестник Моск. ун-та. Сер. 15: Вычислительная математика и кибернетика. – 2017. – № 1. – С. 38–44.

16. Русаловский И.Д. Проблема полностью гомоморфной обработки целых чисел / И.Д. Русаловский, Л.К. Бабенко // Безопасность информации и компьютерных сетей (SIN 2019): матер. 12-й Междунар. науч. конф. – Сочи: Изд-во СГУ, 2019. – С. 41–43.

17. Бабенко Л.К. Библиотека полностью гомоморфного шифрования целых чисел / Л.К. Бабенко, И.Д. Русаловский // Изв. ЮФУ. Технические науки. – 2020. – № 2 (212). – С. 218–227.

Быстревский Сергей Андреевич
Аспирант департамента программной инженерии
и искусственного интеллекта
Дальневосточного федерального университета (ДВФУ)
Аякс пос., 10, о. Русский, г. Владивосток, Россия, 690922
Тел.: +7-908-450-01-70
Эл. почта: serg.by.and97@mail.ru

Боршевников Алексей Евгеньевич
Доцент департамента информационной безопасности ДВФУ
Аякс пос., 10, о. Русский, г. Владивосток, Россия, 690922
ORCID: 0000-0002-7383-1820
Тел.: +7-924-131-67-97
Эл. почта: borshevnikov.ae@dvfu.ru

Добржинский Юрий Вячеславович
Канд. техн. наук, с.н.с., профессор департамента
информационной безопасности ДВФУ
Аякс пос., д. 10, о. Русский, г. Владивосток, Россия, 690922
Тел.: +7-914-792-22-98
Эл. почта: dobrzhinskii.yv@dvfu.ru

Bystrevskii S.A., Borshevnikov A.E., Dobrzhinsky Y.V.

Data verification protocol for a confidential computing scheme with homomorphic encryption

Auction trading systems and Big Data technologies play an important role in modern society. However, as soon as these technologies deal with the finances of their users, there is a need to implement security systems in them to ensure the possibility of data verification. The article proposes a data verification protocol based on the use of homomorphic encryption. A formal safety assessment of the developed protocol is shown, and an analysis from a probabilistic standpoint is carried out.

Keywords: confidential computing, homomorphic encryption, data verification, auction bidding.
DOI: 10.21293/1818-0442-2024-27-2-31-36

References

1. Shelupanov A.A., Bragin D.S., Konev A.A., Permyakov R.A. [Technologies of trusted interaction in the ecosystem of the National Technology Initiative] Sovremennoye obrazovaniye: integratsiya obrazovaniya, nauki, biznesa i vlasti: Materialy mezhdunarodnoy nauchno-metodicheskoy konferentsii [*Modern education: integration of education, science, business and government: Proceedings of the international scientific and methodological conference*], Tomsk, TUSUR Publ., 2022, pt. 2, pp. 15–20 (in Russ.).

2. Bystrevsky S.A., Borshevnikov A.E. [On one algorithm of confidential calculations based on homomorphic encryption for conducting auctions] Molodezh'. Nauka. Innovatsii: Sbornik dokladov 65-y mezhdunarodnoy molodezhnoy nauchno-tekhnicheskoy konferentsii [*Youth. Science. Innovations: Collection of Reports of the 65th International Youth Scientific and Technical Conference.*], Vladivostok, Admiral Nevelskoy Maritime State University Publ., 2023, vol. 1, pp. 143–148.

3. Zagartdinov B.N., Polyakov M.V. [Analysis of the implementation of confidential computing technologies]. *Cybersecurity Issues*, 2023, no. 6 (58), pp. 122–127 (in Russ.).

4. Bereshpolov I.S., Kravchenko Yu.A., Sleptsov A.G. [Data clustering algorithm for protecting confidential information on the Internet] *Izvestiya SFedU. Engineering Sciences*, 2023. no. 3 (233), pp. 74–85 (in Russ.).

5. Schneider T., Zohner M. GMW vs. Yao? Ecient Secure Two-Party Computation with Low Depth. *ACS Sensors*, 2017, vol. 2, no. 8, pp. 1128–1132.

6. Zapechnikov S.V., Shcherbakov A.Yu. [Confidential machine learning based on two-way protocols of secure computing] *IT Security*, 2021. vol. 28, no. 4, pp. 39–51 (in Russ.).

7. Zapechnikov S.V. [Confidential machine learning based on three-way secure computing protocols] *IT Security*, 2022. vol. 29, no. 1, pp. 30–43 (in Russ.).

8. Zapechnikov S.V. [Confidential machine learning based on four-sided secure computing protocols] *IT Security*, 2022, vol. 29, no. 2, pp. 46–56 (in Russ.).

9. Asharovy G, Lindelly Y. A Full Proof of the BGW Protocol for Perfectly Secure Multiparty Computation. *DSPA: Issues of Application of Digital Signal Processing*, 2018, vol. 8, no. 1, pp. 12–17. DOI: 10.1007/s00145-015-9214-4.

10. Al-Bassam M., Sonnino A., Krol M., Psaras I. Airtnt: Fair exchange payment for outsourced secure enclave computations. *arXiv preprint*, 2018, URL: https://arxiv.org/pdf/1805.06411, free (Accessed: July 23, 2024).

11. Bentov I., Ji Y., Zhang F., Li Y., Zhao X., Breidenbach L., Daian P., Juels A. Tesseract: Real-time cryptocurrency exchange using trusted hardware. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1521–1538. DOI: 10.1145/3319535.3363221.

12. Cheng R., Zhang F., Kos J., He W., Hynes N., Johnson N., Juels A., Miller A., Song D. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. *2019 IEEE European Symposium on Security and Privacy (Eu-roS&P)*, 2019, pp. 185–200. DOI: 10.1109/EuroSP.2019.00023.

13. Galal H.S., Youssef A.M. Succinctly verifiable sealed-bid auction smart contract. *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, 2018, pp. 3–19. DOI: 10.1007/978-3-030-00305-0_1.

14. Kazarin O.V. [Development of methods for proactive protection of information systems based on confidential computing] *Information Security Issues*, 2013, no. 3 (102), pp. 68–80 (in Russ.).

15. Varanovsky N.P., Martishin S.A., Khrapchenko M.V., Shokurov A.V. [Threshold schemes of homomorphic encryption and information protection in cloud computing] *Bulletin of the Moscow University. Series 15: Computational Mathematics and Cybernetics*, 2017, no. 1, pp. 38–44.

16. Rusalovsky I.D., Babenko L.K. [The problem of complete homomorphic processing of integers] Bezopasnost' informatsii i komp'yuternykh setey (SIN 2019): Materialy 12-y Mezhdunarodnoy nauchnoy konferentsii [*In the collection: Information and Computer Network Security (SIN 2019). Materials of the 12th International Scientific Conference*], Sochi, Sochi State University Publ., 2019, pp. 41–43.

17. Babenko L.K., Rusalovsky I.D. [Library of complete homomorphic encryption of integers] *Izvestiya SFedU. Engineering Sciences*, 2020, no. 2 (212), pp. 218–227 (in Russ.).

Sergey A. Bystrevskii
Postgraduate student, Department of Software Engineering and Artificial Intelligence, Far Eastern Federal University (FEFU)
10, Ajax Bay, Russky Island, Vladivostok, Russia, 690922
Phone: +7-908-450-01-70
Email: serg.by.and97@mail.ru

Aleksei E. Borshevnikov
Assistant Professor, Department of Information Security FEFU
10, Ajax Bay, Russky Island, Vladivostok, Russia, 690922
ORCID: 0000-0002-7383-1820
Phone: +7-924-131-67-97
Email: borshevnikov.ae@dvfu.ru

Yuri V. Dobrzhinsky
Candidate of Sciences in Engineering, Senior Researcher, Professor, Department of Information Security FEFU
10, Ajax Bay, Russky Island, Vladivostok, Russia, 690922
Phone: +7-914-792-22-98
Email: dobrzhinskii.yv@dvfu.ru