УДК 004.056.5

ОБЗОР ПОДХОДОВ К ПОСТРОЕНИЮ ЗАЩИЩЕННЫХ СХЕМ ЭЛЕКТРОННЫХ АУКЦИОНОВ С ЗАКРЫТЫМИ СТАВКАМИ

Лодыгина П. Ю.[1]
Научный руководитель – канд. техн. наук, доцент Давыдов В. В.[1]
[1]Санкт-Петербургский государственный университет аэрокосмического приборостроения
lodyginap@gmail.com

Введение

Электронные аукционы часто обладают существенными практическими преимуществами относительно классических: они, как правило, требуют меньше финансовых вложений и доступны участникам независимо от местоположения. Вместе с тем электронный формат требует усиленных мер безопасности и контроля корректности проведения торгов. Участники онлайн-аукционов в большинстве своем заинтересованы в сохранении конфиденциальности своих данных, так как эти данные могут быть использованы как организаторами, так и другими участниками в ущерб их интересам. Из-за этого появляется необходимость в реализации аукционов с закрытыми ставками (sealed-bid). В аукционах данного формата участники передают свои ставки в скрытом виде, причем их значения недоступны как организатору, так и остальным участникам. После получения всех ставок определяются наибольшая и ее владелец, при этом должна обеспечиваться приватность ставок проигравших участников.

В ряде практических сценариев организатор торгов не рассматривается как полностью доверенная сторона, в связи с чем требуется построение протоколов, обеспечивающих честность и приватность без раскрытия ставок, что может быть обеспечено с использованием криптографических примитивов.

Основная часть

В работе приводится сравнительный обзор наиболее распространенных подходов к построению онлайн-аукционов с закрытыми ставками. В первую очередь рассматриваются вычислительная сложность протокола и удобство его использования для участников. Приватность ставок проигравших участников считается обязательным требованием, а основные свойства – устойчивость к недобросовестному поведению участников и организатора, невозможность отзыва или изменения ранее зафиксированной ставки и публичная проверяемость результата [1] – как правило достигаются за счет дополнительных примитивов.

Наиболее универсальным подходом представляется использование протоколов конфиденциальных вычислений (MPC) для совместного определения наибольшей ставки без раскрытия остальных [2]. Однако интерактивная природа протоколов совместных вычислений может быть неудобна в практических сценариях. Стоит также отметить снижение эффективности с ростом числа участников аукциона, так как поиск максимума в MPC считается «тяжелой» операцией и реализуется, как правило, посредством композиции попарных сравнений. Для повышения эффективности могут применяться схемы гомоморфного разделения секрета, поддерживающие сравнение [3], что позволит сократить количество взаимодействий по сравнению с универсальными протоколами конфиденциальных вычислений.

Другой подход состоит в предварительной фиксации своей ставки участниками с использованием, например, неотрицаемой групповой подписи [4] или схемы обязательств [5]. После этого организатор оглашает ставки «на понижение» до тех пор, пока не найдется участник, зафиксировавший в качестве ставки нынешнюю цену (или

чуть большую названной) и предоставивший доказательство этого. Очевидно, подобный формат аукциона требует присутствия участника в сети во время проведения торгов, из-за чего неудобен для электронного формата.

Ещё одним вариантом реализации аукциона является предварительная публикация организатором допустимого ценового диапазона и формирование каждым участником вектора ставок через присвоение нулевых значений всем элементам, соответствующим ценам выше выбранной ставки и ненулевых – остальным. В таком случае для каждой отдельной цены может быть определено, существует ли участник, готовый заплатить данную сумму, после чего максимальная ставка определяется с помощью бинарного поиска. Данный подход реализуется с использованием гомоморфного шифрования с пороговым разделением ключа [6], но на практике часто используется аддитивная гомоморфность схемы разделения секрета Шамира [7], позволяющая с минимальными взаимодействиями определить сумму секретов без раскрытия отдельных значений; применение проверяемого разделения секрета (VSS) обеспечивает устойчивость в модели активного злоумышленника.

Стоит отметить, что достижение желаемых свойств безопасности обычно не обеспечивается использованием одного базового примитива. Для реализации проверяемости результатов часто применяют публичные доски, на которых публикуются промежуточные результаты вычислений. Для гарантии неизменяемости ставки используются схемы обязательств совместно с электронной подписью, а корректность определения победителя и некоторых отдельных этапов подтверждается через доказательства с нулевым разглашением.

Выводы

В работе исследованы принципы построения схем приватных аукционов с закрытыми ставками. Проведенный анализ показал, что подход с представлением ставки в векторном виде совместно с разделением секрета представляется наиболее практичным, так как обеспечивает высокий уровень стойкости при умеренной вычислительной сложности и сравнительно низкой интерактивности.

Литература

1. Alvarez R., Nojoumian M. Comprehensive survey on privacy-preserving protocols for sealed-bid auctions // Computers & Security. – 2020. – Т. 88. – С. 101502.
2. Cachin C. Efficient private bidding and auctions with an oblivious third party // Proceedings of the 6th ACM Conference on Computer and Communications Security. – 1999. – С. 120-127.
3. Deng W. et al. MORSE: An Efficient Homomorphic Secret Sharing Scheme Enabling Non-Linear Operation // arXiv preprint arXiv:2410.06514. – 2024.
4. Sakurai K., Miyazaki S. An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme: –On the importance of hiding the winner’s identity against bid-rigging– // Australasian Conference on Information Security and Privacy. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2000. – С. 385-399.
5. Nojoumian M., Stinson D. R. Unconditionally secure first-price auction protocols using a multicomponent commitment scheme // International Conference on Information and Communications Security. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2010. – С. 266-280.
6. Peng K., Dawson E. Efficient bid validity check in elgamal-based sealed-bid e-auction // International Conference on Information Security Practice and Experience. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2007. – С. 209-224.
7. Peng K., Boyd C., Dawson E. Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing // International Conference on Cryptology in Malaysia. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2005. – С. 84-98.