OUKA
The University of Osaka
Institutional Knowledge Archive

Title	Scalable and Public Verifiable M+1st-Price Auction on Smart Contract
Author(s)	許, 伯駒
Citation	大阪大学, 2023, 博士論文
Version Type	
URL	https://hdl.handle.net/11094/95919
rights	
Note	やむを得ない事由があると学位審査研究科が承認したため、全文に代えてその内容の要約を公開しています。全文のご利用をご希望の場合は、大阪大学の博士論文についてをご参照ください。

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

Form 3

Abstract of Thesis

Name （許 伯駒）

Title: Scalable and Public Verifiable M+1st-Price Auction on Smart Contract
（スケーラブルかつ公開検証可能なスマートコントラクトを用いたM+1値入札システム）

Based on highly developed internet technology, online services have become a trend. Security plays an important role in protecting hackers' threats. In the government, the selection of vendors shall be made by sealed-bid auction. Each bid is sealed by the bidder and sent to a manager. The manager is trusted to announce the winning bidder without revealing each bidder's bid. A second-price auction, where the bid price reflects the bidder's idea of value, won the Nobel Prize. In a second-price sealed-bid auction, the winning bidder pays the second-highest bidding price to buy the goods. Google Ads used a second-price sealed-bid auction but migrated to an English auction (the winner pays the highest price) because it is not easy to achieve public verifiability on the second price when all bids are sealed. A second-price auction can be generalized to a M+1st-price auction that sells M goods. The following four properties are required: correctness, public verifiability, bid secrecy, and M+1st-bidder's anonymity. In this dissertation, the following three protocols that fulfills all required properties are proposed.

In the first study, a Smart Contract based auction protocol without a trusted manager is proposed. The Blockchain can executes the the Smart Contract honestly to ensure correctness. Public verifiability can be ensured by zero-knowledge proofs. The Smart Contract verifies the proofs to make sure each bidder follows the protocol. If a bidder cannot provide valid zero-knowledge proof, the bidder will be considered malicious. At the beginning of the auction, all bidders need to send some money as a stake to the auction contract. When malicious behavior is detected, the malicious bidder's stake will be used to compensate all other honest bidders. The only problem is the storage in a Smart Contract is public. As a result, this study propose a multi-party ElGamal encryption to ensure bid secrecy. The multi-party ElGamal encryption allows each bidder to encrypt their bidding vector by all bidders' public keys. Unless all bidders collaborate, a malicious bidder cannot learn any information.

In the second study, an auction protocol that reached optimal time complexity O(|V|) per bidder is proposed. In the first study, the time complexity of each bidder is O(BM|V|). The B factor is mainly caused by the design that each bidder needs to check all other bidders' bids. To remove the B factor, all algorithms that need all bidders' collaboration are replaced by zero-knowledge proofs. The M factor is mainly caused by the usage of Mix and Match to keep the M+1st-bidder's anonymity. To remove the M factor, a greedy strategy that when there's no tie, a Mix and Match is not necessary is realized. This study propose a zero-knowledge algorithm that can find the M+1st-price in O(1) time while keeping the M+1st-bidder's anonymity. To further reduce the constants, this study found the EIP-196 prebuild functions can be used to speed up the zero-knowledge proof verification in Smart Contracts. The computation cost is reduced by 95%. By using the findings explained above, this study can reach the optimal time complexity O(|V|) per bidder.

In the third study, an auction protocol that has an exponential level bid upper bound is proposed. To reach 2^|V| - 1 bid upper bound, a binary format bidding vector is necessary. Each bidder's bid is encoded in a base 2 binary format. To keep bid secrecy and the M+1st-bidder's anonymity, homomorphic AND and homomorphic OR algorithms are necessary. This study propose a zero-knowledge AND proof to replace the homomorphic AND operation. By using this zero-knowledge proof, this study do not need a homomorphic multiplication at all. The homomorphic addition property given by ElGamal encryption is sufficient. The techniques used in the second study is also used to remove the B factor from the time complexity. As a result, this proposal extends the bid upper bound to an exponential level without a SHE or FHE for the first time.

In this dissertation, auction protocols without a trusted manager, reaches the optimal time complexity and extends the bid upper bound to an exponential level are proposed for the first time.

様式７

論文審査の結果の要旨及び担当者

氏　名　（　許 伯駒　　）

	（職）	氏　　名
論文審査担当者		
主 査	教授	宮地　充子
副 査	教授	滝根　哲哉
副 査	教授	丸田　章博
副 査	教授	井上　恭
副 査	教授	田中　雄一
副 査	教授	鷲尾　隆
副 査	教授	駒谷　和範
副 査	講師	王 イントウ
副 査	教授	Joseph Liu（Monash University Department of Software Systems & Cybersecurity）

論文審査の結果の要旨

Our society has become increasingly digitalized, and thus online services have become a trend. Recently, auctions even in a government to select vendors are often done electronically rather than on paper. Security plays an important role in protecting confidential information. There are several types of auctions such as sealed-bid auction, a second-price sealed bid auction, etc. In a second-price sealed-bid auction, the winner gets a target good with the second-highest, whose strategy won the Nobel Prize. Because the second-price auctions have been shown to be the best strategy for both sellers and buyers, as buyers are shown to bid at the price they can afford. For this reason, it is economically desirable to be able to conduct second-price auctions. However, there are significant difficulties in implementing second-price auctions electronically. In second-price auctions, any bid value except the 2nd price as well as the highest value and 2nd bidder should be secret, which are called bid secrecy and 2nd-bidder's anonymity. Furthermore protocol itself needs to prove that the winner bids in the highest value and pays in the second value, which is called public verifiability. A second-price auction can be generalized to a M+1st-price sealed-bid auction that sells M items, which also requires bid secrecy and 2nd-bidder's anonymity, and public verifiability. Easiest way to achieve such a M+1-st price auction is to introduce the trusted third party (TTP), in which TTP manages procedures and prove that the winner bids in the highest value and pays in the second value since TTP knows all bidders' value. Unfortunately, there has not been proposed efficient M+1st-price sealed-bid auctions without using TTP. In this dissertation, secure and efficient M+1st-price sealed-bid auctions are studied. This dissertation consists of the following three contributions.

1. An auction protocol without a trusted manager.

In this research, bids are represented by bid vector V to achieve efficiency, Then the number of available bids is the vector size |V|. In addition, to construct an auction protocol without TTP, a Smart Contract a protocol is introduced. The Smart Contract verifies the zero-knowledge proofs to ensure public verifiability. If a bidder cannot provide valid zero-knowledge proof, the bidder is considered malicious. When malicious behavior is detected, the malicious bidder's stake will be used to compensate all other honest bidders. The only problem of using a Smart Contract is that it cannot hide any secrets. To resolve the problem, multi-party ElGamal encryption was introduced to ensure bid secrecy and the M+1st-bidder's anonymity. The multi-party ElGamal encryption allows each bidder to encrypt their bidding vector by all bidders' public keys. Unless all bidders collaborate, a malicious bidder cannot learn any information. As for the performance, the time complexity is O(BM|V|) per bidder and the number of bids is |V|, where B is the number of bidders.

2. Auction Protocol with Optimal Complexity

In this research, an auction protocol with optimal time complexity O(|V|) per bidder was achieved. To remove the B factor from the first research, an approach that uses zero-knowledge proofs was introduced to replace all algorithms. To remove the M factor, a greedy strategy was introduced. As a result, as long as there's no tie, a Mix and Match is removed. A new zero-knowledge algorithm that can find the M+1st-price in O(1) time was also proposed while keeping the M+1st-bidder's anonymity. In addition to time complexity, practical time was further reduced by using the EIP-196 prebuild functions, which speed up the zero-knowledge proof verification in Smart Contracts. As for the performance, the time complexity is O(|V|) per bidder and the number of bids is |V|.

3. Auction Protocol with Exponential Upper Bound

In this research, the number of bids |V| is increased to $2^{|V|}$. To extend the number of bids, a base 2 format is used to encode the bidding vector. Since a homomorphic AND and a OR operation are necessary to compare base 2 format secret values, a zero-knowledge proof (ZKP) that each bidder can prove the result of a homomorphic AND operation was newly proposed. By using the ZKP, only partially homomorphic encryption such as an ElGamal encryption is used to perform a homomorphic OR operation. As for the performance, the time complexity is O(M|V|) per bidder and the number of bids is $2^{|V|}$. Comparing to the second construction, time complexity is larger but the number of bids becomes increased. Therefore users can choose the 2nd or 3rd auction according to their situations.

As described above, in this dissertation, secure and efficient M+1st-price sealed-bid auctions are realized by applying

multi-party encryption, zero-knowledge proof, and binary format bidding vector. Auction theory also won the Nobel Prize in Economics in 2020. As society becomes increasingly digitalized, electronic auctions are expected to become increasingly important. Then, this thesis will contribute to the realization of secure and efficient electronic auctions. The impact of this research on the further digitalization of governments is immeasurable.

Therefore, this thesis contributes significantly to the development of the field of information security and engineering and is recognized as a valuable doctoral dissertation.