Theoretical Computer Science 730 (2018) 44–92

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Secret, verifiable auctions from elections

Elizabeth A. Quaglia [a,*], Ben Smyth [b]

[a] Information Security Group, Royal Holloway, University of London, United Kingdom
[b] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg

ARTICLE INFO

Article history:
Received 25 October 2017
Received in revised form 7 February 2018
Accepted 17 March 2018
Available online 23 March 2018
Communicated by G. Persiano

Keywords:
Auctions
Elections
Privacy
Secrecy
Verifiability

ABSTRACT

Auctions and elections are seemingly disjoint. Nevertheless, similar cryptographic primitives are used in both domains. For instance, mixnets, homomorphic encryption and trapdoor bit-commitments have been used by state-of-the-art schemes in both domains. These developments have appeared independently. For example, the adoption of mixnets in elections preceded a similar adoption in auctions by over two decades. In this paper, we demonstrate a relation between auctions and elections: we present a generic construction for auctions from election schemes. Moreover, we show that the construction guarantees secrecy and verifiability, assuming the underlying election scheme satisfies analogous security properties. We demonstrate the applicability of our work by deriving auction schemes from the Helios family of election schemes. Our results advance the unification of auctions and elections, thereby facilitating the progression of both domains.

1. Introduction

We present a construction for auction schemes from election schemes, and prove the construction guarantees security, assuming the underlying election scheme is secure.

Auctions An auction is a process for the trade of goods and services from sellers to bidders [53,65], with the support of an auctioneer. We study first-price sealed-bid auctions [15], whereby bidders create bids which encapsulate the price they are willing to pay, and the auctioneer opens the bids to determine the winning price (namely, the highest price bid) and winning bidder.

Elections An election is a decision-making procedure used by voters to choose a representative from some candidates [44, 3], with the support of a tallier. We study first-past-the-post secret ballot elections [63,75], which are defined as follows. First, each voter creates a ballot which encapsulates the voter's chosen candidate (i.e., the voter's vote). Secondly, all ballots are tallied by the tallier to derive the distribution of votes. Finally, the representative – namely, the candidate with the most votes – is announced.

Bidders and voters should express their choice freely in auctions and elections; this can be achieved by participating in private [71,95,94,69], which has led to the emergence of the following requirements.

- Bid secrecy: A losing bidder cannot be linked to a price.

* Corresponding author.
E-mail address: elizabeth.quaglia@rhul.ac.uk (E.A. Quaglia).

https://doi.org/10.1016/j.tcs.2018.03.022
0304-3975/

- Ballot secrecy: A voter cannot be linked to a vote.

Ballot secrecy aims to protect the privacy of all voters, whereas bid secrecy is only intended to protect the privacy of losing bidders. This intuitive weakening is necessary, because the auctioneer reveals the winning price and winning bidder, hence, a winning bidder can be linked to the winning price.

Bidders and voters should be able to check that auctions and elections are run correctly [49,37,34,1,2,38]; this is known as *verifiability*. Sometimes we write *auction verifiability* and *election verifiability* to distinguish verifiability in each field. Kremer, Ryan and Smyth [54] decompose verifiability into the following properties.

- Individual verifiability: bidders/voters can check whether their bid/ballot is included.
- Universal verifiability: anyone can check whether the result is computed properly.

Conceptually, individual and universal verifiability do not differ between auctions and elections.

1.1. Constructing auctions from elections

Our construction for auction schemes from election schemes works as follows.

1. We represent prices as candidates, and instruct bidders to create bids by "voting" for the candidate that represents the price they are willing to pay.
2. Bids are "tallied" to derive the distribution of prices and the winning price is determined from this distribution.

The relation between auctions and elections is so far straightforward. The challenge is to establish the winning bidder. This is non-trivial, because election schemes satisfying ballot secrecy ensure voters cannot be linked to votes, hence, the bidder mentioned above cannot be linked to the price they are willing to pay. We overcome this by extending the tallier's role to additionally reveal the set of ballots for a specific vote,[1] and exploit this extension to complete the final step.

3. The tallier determines the winning bids and a winning bidder can be selected from these bids.[2]

Extending the tallier's role is central to our construction.

1.2. Motivation and related work

There is an abundance of rich research on elections which can be capitalised upon to advance auctions. This statement can be justified with hindsight: Chaum [32] exploited mixnets in elections twenty-three years before Peng et al. [72] made similar advances in auctions (Jakobsson and Juels [51] use mixnets in a distinct way from Chaum and Peng et al.), Benaloh and Fischer [25] proposed using homomorphic encryption seventeen years before Abe and Suzuki [5], and Okamoto [70] demonstrated the use of trapdoor bit-commitments six years before Abe and Suzuki [6].

Magkos, Alexandris and Chrissikopoulos [64] and Her, Imamot and Sakurai [46] have studied the relation between auctions and elections. Magkos, Alexandris and Chrissikopoulos remark that auctions and elections have a similar structure and share similar security properties. And Her, Imamot and Sakurai contrast privacy properties of auctions and elections, and compare the use of homomorphic encryption and mixnets between fields. More concretely, McCarthy, Smyth and Quaglia [67] derive auction schemes from the Helios and Civitas election schemes. And Lipmaa, Asokan and Niemi study the converse [62, §9].

1.3. Contribution

We *formally* demonstrate a relation between auctions and elections: we present a generic construction for auction schemes from election schemes, moreover, we prove that auction schemes produced by our construction satisfy bid secrecy and auction verifiability, assuming the underlying election scheme satisfies ballot secrecy and election verifiability. To achieve this, we formalise syntax and security definitions for auction schemes, since these are prerequisites to rigorous, formal results.

Summary of contributions and paper structure We summarise our contributions as follows.

- We propose auction scheme syntax, and the first computational security definitions of bid secrecy and verifiability for auctions (§2).

[1] Ballot secrecy does not prohibit such behaviour, because ballot secrecy assumes the tallier is trusted.

[2] Handling tie-breaks (i.e., selecting a winning bid from a set of winning bids) is straightforward. For instance, the set could be sampled uniformly at random. So this paper does not address this problem.