史闻博　王佳琪◎著

# 面向电子拍卖的安全计算技术与协议研究

科学出版社

# 面向电子拍卖的安全计算技术与协议研究

史闻博　王佳琪　著

科学出版社

北京

## 内 容 简 介

本书主要讲述面向电子拍卖安全计算研究的安全技术和应用范例，主要内容包括：电子拍卖的概述、数字签名技术在电子拍卖中的应用、加密技术在电子拍卖中的应用、安全多方计算在电子拍卖中的应用以及拍卖中的协议安全分析与证明。

本书面向对电子拍卖安全技术感兴趣的计算机专业的本科生或研究生，以及在电子拍卖安全技术领域潜心研究的科学工作者。本书还可以作为高等院校相关专业学生、研究人员以及工程实践人员的参考书。

**图书在版编目（CIP）数据**

面向电子拍卖的安全计算技术与协议研究 / 史闻博，王佳琪著. —北京：科学出版社，2018.9

ISBN 978-7-03-056065-0

Ⅰ. ①面… Ⅱ. ①史… ②王… Ⅲ. ①互联网络-应用-拍卖-安全技术-研究 Ⅳ. ①F713.359-39

中国版本图书馆 CIP 数据核字（2017）第 314753 号

责任编辑：王喜军 / 责任校对：王 瑞
责任印制：吴兆东 / 封面设计：壹选文化

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http：//www.sciencep.com

北京虎彩文化传播有限公司印刷
科学出版社发行 各地新华书店经销
*
2018 年 9 月第 一 版 开本：720×1000 1/16
2018 年 9 月第一次印刷 印张：9 1/4
字数：180 000

**定价：98.00 元**

（如有印装质量问题，我社负责调换）

# 前　言

电子拍卖安全计算研究是信息安全领域的一个重要应用，但目前大多数信息安全相关的教材与专著都过于偏重信息安全技术的讲解，而忽略了对实际场景的具体应用，并且没有一本书详细地介绍电子拍卖领域的安全计算研究。基于此，本书将信息安全技术与电子拍卖应用实例相结合，首先了解信息安全技术的相关基础知识，再循序渐进地引入电子拍卖安全的相关实例，使读者可以逐步了解电子拍卖安全的整个安全技术体系。

本书共 5 章。第 1 章为绪论，介绍电子拍卖的一些基础知识，包括电子拍卖的定义、电子拍卖系统应具有的特性、电子拍卖的主要形式、电子拍卖的类型、电子拍卖的模型以及电子拍卖决策计算面临的安全问题。第 2 章介绍数字签名技术在电子拍卖中的应用，包括普通数字签名技术及其应用实例和特殊数字签名技术及其应用实例。普通数字签名技术分为 RSA 数字签名技术、ElGamal 数字签名技术；特殊数字签名技术分为群签名技术、盲签名技术、环签名技术。第 3 章介绍加密技术在电子拍卖中的应用，包括 ElGamal 加密系统及其应用实例、Paillier 加密系统及其应用实例以及椭圆曲线加密系统及其应用实例。第 4 章介绍安全多方计算在电子拍卖中的应用，包括不经意传输技术及其应用实例、秘密共享机制及其应用实例、比特承诺技术以及姚氏百万富翁问题及其应用实例。第 5 章介绍拍卖中的协议安全分析与证明，包括可证明安全理论方法、安全多方计算理论与方法、零知识证明理论与方法、形式化分析以及电子拍卖的安全特性分析。这些内容涵盖了安全电子拍卖所涉及的安全技术研究和应用实例。为了便于读者学习，本书在编写过程中尽量做到结合实际，文字力求通俗易懂，在书中使用了大量的实例帮助读者理解。

本书的出版得到了国家自然科学基金项目（编号：61472074，U1708262）、

中央高校基本科研业务费项目（编号：N172304023）和东北大学秦皇岛分校科研专著专项基金项目的支持和资助，在此表示感谢。

安全计算相关的技术发展非常快，新思想、新观点不断涌现，本书虽力求全面地介绍电子拍卖的安全计算技术与协议，但由于作者水平有限，加之时间仓促，书中难免会有不妥之处，殷切希望广大读者批评指正。

作　者

2017 年 12 月

# 目　录

# 第1章 绪　论

## 1.1 拍卖交易的历史

### 1.1.1 世界拍卖交易历史

人类历史上最早的拍卖活动是关于试婚女子的拍卖，最早记录在“历史之父”希罗德的《历史》一书中[1]。古巴比伦人将适龄女子聚集到一处，男子则在她们外面站成一个圆圈，然后拍卖人按次序把她们出卖。富人若是想要娶得最漂亮的姑娘就要相互出价竞争。而在这一过程当中，主持拍卖的临时拍卖人则为世界历史上出现最早的拍卖人。

从罗马共和时期到罗马帝国时期，拍卖开始逐渐兴盛起来，通过战争，拍卖产业发展到鼎盛时期，大量的商人随军出征，商人买下士兵手中的战利品进行倒卖从中赚取差价，而世界拍卖行业从欧洲的中世纪开始步入衰落时期，这是封建主义阶级垄断了生产的结果。这一时期拍卖受到了各种制约，一直到16世纪中叶才开始陆续出现拍卖活动。进入18世纪，1744年成立的苏富比拍卖行和1766年成立的佳士得拍卖行成为世界上最大的两个拍卖行。19世纪末，两家拍卖行都进入了鼎盛时期，几乎垄断了整个拍卖市场。到20世纪初，全世界从事拍卖销售工作以及拍卖形式销售货物的总人数已经非常惊人，这也为拍卖行业的发展创造了今天的大好形势，也使得拍卖行业融入各个领域中。

### 1.1.2 中国拍卖交易历史

中国最早的拍卖活动是魏晋时期寺院通过“唱衣”的方式将去世僧人的衣物和贡品进行拍卖。寺院通过拍卖的方式筹集维持经济的善款。唐朝时期的《通典》一书中记载的拍卖与现代拍卖的意义已经有了共同之处。

中国长期处于封建社会，在这种自给自足的自然经济条件下，商品生产规模及交换关系非常有限，导致拍卖行业发展极为缓慢。然而当西方人的剩余物资大批占领中国市场的同时，他们也给中国带来了他们最喜欢的交易方式——拍卖。在中国古代的沿海等地区，建立了较大的拍卖中心，使得拍卖交易得到普遍的发展。20 世纪 80 年代后期，中国拍卖行业得到了恢复和长足的发展。中国走上了经济体制改革的道路，社会主义市场经济体制得到了逐步确立和完善，拍卖作为市场经济的一种流通手段开始恢复经营并得到了良好的发展。拍卖交易在人们日常生活中的地位也越来越显著。1997 年出台的《中华人民共和国拍卖法》将拍卖定义为：以公开竞价的方式，将特定的物品或财产权利转让给最高应价者的买卖方式。公开、公平、公正及诚实、信用为拍卖活动必须遵守的基本原则。通过不断地发展，中国拍卖行业已经广泛涉猎文物、金融、铁路、商贸、土地等多个领域，涉及行业十余项。进入 21 世纪，中国拍卖行业进入了稳步发展时期。

## 1.2 拍卖的方式

拍卖的方式有英格兰式拍卖（English auction）、荷兰式拍卖（Dutch auction）、英格兰式与荷兰式结合式拍卖、密封递价式拍卖、标准增量式拍卖等。

### 1.2.1 英格兰式拍卖

英格兰式拍卖，也称增价拍卖或低估价拍卖，是指在拍卖过程中，拍卖人宣布拍卖标的的起叫价及最低增幅，竞买人以起叫价为起点，由低至高竞相应价，最后以最高竞价者三次报价无人应价后，响槌成交。但成交价不得低于保留价。

### 1.2.2 荷兰式拍卖

荷兰式拍卖，也称降价拍卖或高估价拍卖，是指在拍卖过程中，拍卖人宣布拍卖标的的起拍价及降幅，并依次叫价，第一位应价人响槌成交。但成交价不得低于保留价。

### 1.2.3 英格兰式与荷兰式结合式拍卖

英格兰式与荷兰式结合式拍卖，是指在拍卖过程中，拍卖人宣布起拍价及最低增幅，由竞买人竞相应价，拍卖人依次升高叫价，以最高应价者竞得。若无人应价则转为拍卖人依次降低叫价及降幅，并依次叫价，以第一位应价者竞得。但成交价不得低于保留价。

### 1.2.4 密封递价式拍卖

密封递价式拍卖，又称招标式拍卖。由买主在规定的时间内将密封的报价单（也称标书）递交拍卖人，由拍卖人选择买主。这种拍卖方式和英格兰式与荷兰式这两种方式相比较有以下两个特点：一是除价格条件外，还可能有其他交易条件需要考虑；二是可以采取公开开标方式，也可以采取不公开开标方式。拍卖大型设施或数量较大的库存物资或政府罚没物资时，可能采用这种方式。

### 1.2.5 标准增量式拍卖

标准增量式拍卖是一种拍卖标的数量远大于单个竞买人的需求量而采取的一种拍卖方式（此拍卖方式非常适合大宗积压物资的拍卖活动）。卖方为拍卖标的设计一个需求量与成交价格的关系曲线。竞买人提交所需标的的数量之后，如果接受卖方根据他的数量而报出的成交价即可成为买受人。

### 1.2.6 维克瑞式拍卖

维克瑞式拍卖，也称为第二价格密封拍卖。这种拍卖方式与首价密封拍卖基本相同，区别仅在于胜出者需要支付的价格是第二高的报价，而不是他自己的报价。这与易趣网所使用的代理人竞价系统相似，在这个系统中，胜出者需要支付第二高的报价，再加上一个报价的增额。

### 1.2.7　速胜式拍卖

速胜式拍卖是增价式拍卖的一种变体。拍卖标的物的竞价也是按照竞价阶梯由低到高、依次递增，不同的是，当某个竞买人的出价高于或等于保留价时，拍卖结束，此竞买人成为买受人。

### 1.2.8　反向拍卖

反向拍卖也称为逆向拍卖，常用于政府采购、工程采购等。由采购方提供希望得到的产品的信息、需要服务的要求和可以承受的价格定位，由卖家之间以竞争方式决定最终产品提供商和服务供应商，从而使采购方以最优的性能价格比实现购买。

### 1.2.9　定向拍卖

定向拍卖是一种为特定的拍卖标的物而设计的拍卖方式，有意竞买者必须符合卖家所提出的相关条件才可成为竞买人参与竞价。

## 1.3　电子拍卖的定义及优势

### 1.3.1　电子拍卖的定义

电子拍卖是传统拍卖形式的在线实现。卖方可以借助网上拍卖平台运用多媒体技术来展示自己的商品，这样就可以免除传统拍卖中实物的移动；竞标者也可以借助网络，足不出户进行网上竞标。通常，电子拍卖是和电子签约、电子支付整合应用的。一般地，在进行电子拍卖前，拍卖方会在网上发布拍卖品的详细信息和拍卖规则，必要时可通过多媒体展示拍卖品；在某些情况下，会要求有意竞标者预先报名，并对竞标者的资格进行审查，这些程序也是通过网络进行的。拍卖正式开始后，竞标者在网上进行竞标。

### 1.3.2 电子拍卖的优势

与传统拍卖相比，电子拍卖具有以下优势。

（1）网上交易成本低，各种新品或二手商品都可以在网上进行电子拍卖。拍卖可以充分地利用手中的资源，减少了不需要的东西。买方以较低的价格和交易的费用就可以买到自己需要的东西。

（2）电子拍卖可以通过数码照片、视频资料等多媒体手段为客户展示拍卖物品的大小、样式、性能，使得客户对于物品能够先有一定的了解。

（3）电子拍卖在服务功能上并不比传统拍卖市场逊色，它能够提供与拍卖相配套的系列服务，如达成交易、支付货款以及办理运输等。

随着网络的普及化，电子拍卖将具有非常广阔的应用前景。

## 1.4 电子拍卖系统应具有的特性

### 1.4.1 竞标者的匿名性

从拍卖开始到拍卖结束，当拍卖结果公开之后，包括可信权威机构的任何成员都不能获得竞拍失败人的任何身份信息以及投标失败人的投标出价。因此，竞标者具有匿名性。

### 1.4.2 获胜竞标者的不可抵赖性

从拍卖开始到拍卖结束，当拍卖决出获胜的竞标者时，竞标者不能否认其已经提交的最高出价，并且可以确切地获得竞标者的身份信息。因此，获胜竞标者具有不可抵赖性。

### 1.4.3 拍卖的公开验证性

当拍卖结束之后，任何人都可以公开地验证获胜者即竞胜者的有效性，通过

有效的验证确认获胜竞标者的确是所有竞标者当中最高的出价方。因此，拍卖具有公开验证性。

### 1.4.4　拍卖的不可欺骗性

在拍卖过程中，任何人都不能伪装成某个已经注册的竞标者进行竞价。因此，拍卖具有不可欺骗性。

### 1.4.5　协议健壮性

在拍卖过程中，即使竞标者提交一个无效的投标，拍卖过程也不会受到任何影响，因此，拍卖协议具有健壮性。

### 1.4.6　拍卖的高效性

在英式电子拍卖中拍卖的效率是非常重要的，因为竞标者实时出价，所以英式电子拍卖协议主要是为了提高拍卖的效率，拍卖过程的验证投标书及撤销竞标者的计算量和通信量应适合实际使用。

## 1.5　电子拍卖的主要形式

电子拍卖有以下三种形式：英格兰式拍卖、最高价秘密投标、最二高价秘密投标。

### 1.5.1　英格兰式拍卖（电子拍卖）

英格兰式拍卖是最普遍的一种交易形式。用户竞出他们乐意出的最高价，交易期限一到，交易同时停止，物品将卖给出价最高者。

### 1.5.2　最高价秘密投标

最高价秘密投标是指，买主在竞拍开始后将标书密封形式投标，在卖家宣布投标结束后打开标书，与出价最高者成交。

### 1.5.3 最二高价秘密投标

最二高价秘密投标也是一种密封投标方式，不同之处在于最高出价者是以第二高出价者所出价格买走交易品。

## 1.6 电子拍卖的类型

电子拍卖按不同标准可以分为不同类型，本节主要介绍以下几种常用的类型。

### 1.6.1 一次拍卖和再拍卖

按拍卖次数不同可以分为一次拍卖和再拍卖。一次拍卖是指只经过一次拍卖就拍定的拍卖。再拍卖是指必须经过两次及两次以上的程序才拍定的拍卖。

### 1.6.2 增价拍卖和减价拍卖

按价格递增或递减可以分为增价拍卖和减价拍卖。增价拍卖指的是前面提到的英格兰式拍卖，也称为低估价拍卖，是指在拍卖过程中，拍卖人宣布拍卖标的的起叫价及最低增幅，竞买人以起叫价为起点，由低至高竞相应价，最后以最高竞价者三次报价无人应价后，响槌成交，但成交价不得低于保留价。减价拍卖又称为荷兰式拍卖，也称为高估价拍卖，是指在拍卖过程中，拍卖人宣布拍卖标的的起叫价及降幅，并依次叫价，第一位应价人响槌成交，但成交价不得低于保留价。

### 1.6.3 有底价拍卖和无底价拍卖

拍卖按是否有底价又可以分为有底价拍卖和无底价拍卖。有底价拍卖是指拍卖前设定最低售价或者保留价的拍卖。无底价拍卖是指拍卖前不设置最低价或保留价的拍卖。

### 1.6.4　投标式拍卖和非投标式拍卖

拍卖按是否公开的形式又可以分为投标式拍卖和非投标式拍卖。投标式拍卖又称密封递价式拍卖，是反映拍卖人事先公布拍卖标的相关情况以及拍卖条件，其中又有公开底价和不公开底价两种形式，但竞买人均在规定时间内将其竞价载入密封标单交给拍卖人，再由拍卖人在规定时间内统一开标，择优选取中标者。非投标式拍卖是指普通拍卖，即公开形式的拍卖。

### 1.6.5　单属性拍卖和多属性拍卖

按拍卖商品属性的个数不同，拍卖又可以分为单属性拍卖和多属性拍卖。单属性拍卖指的是在单个商品的拍卖中，买卖双方只对物品价格这一属性感兴趣的拍卖。通常网上的电子拍卖类型都指的是单属性拍卖。在实际交易的过程当中，买卖双方不仅对双方的价格感兴趣，还需考虑其他属性因素，如提交时间、各种质量参数、售后服务的内容等，并且，通常买方对不同属性的物品估价不同，而卖方产生的不同属性物品所需的成本也不同，买方估价值和卖方成本均可看做物品属性的函数。能够使买卖双方在物品的各种属性上进行协商的拍卖方法称为多属性拍卖。

### 1.6.6　特殊类型的拍卖

还有一些特殊类型的拍卖，具体如下。

1. 频谱拍卖

频谱拍卖根据其自身的特点，使得拍卖机制与其他传统拍卖略有不同。频谱拍卖指的是一种十分公平高效的频谱分配方式，频谱拍卖中，频谱可以通过竞价的方式获得自己需要的通信信道，主用户也可以通过出租信道得到一定的