第 35 卷 第 8 期 计 算 机 工 程 2009 年 4 月
Vol.35 No.8 Computer Engineering April 2009
·安全技术· 文章编号：1000—3428(2009)08—0164—02 文献标识码：A 中图分类号：TP309.2

基于 Hash 链的电子拍卖安全性分析及改进

肖自碧[1]，杨 波[2]，李寿贵[1]
(1. 武汉科技大学理学院，武汉 430081；2. 北京邮电大学信息安全中心，北京 100876)

摘 要：基于 Hash 链的电子拍卖方案具有技术简单和计算效率高的优势。分析杨加喜等人提出的一种基于 Hash 链的电子拍卖方案(计算机工程，2007 年第 19 期)的安全性缺陷，在其基础上提出具有不可伪造性、不可否认性、时限性、投标者匿名性以及抗合谋攻击的改进方案，并提出进一步的研究思想。

关键词：密封式拍卖；Hash 函数；Hash 链

Security Analysis and Improvement of Electronic Auction Based on Hash Chain

XIAO Zi-bi[1], YANG Bo[2], LI Shou-gui[1]
(1. School of Science, Wuhan University of Science and Technology, Wuhan 430081;
2. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876)

【Abstract】Electronic auctions based on Hash chain have advantages over non Hash-based schemes due to the simplicity and efficiency of Hash chain. Security flaws of a new electronic auction based on hash chain presented by Yang Jiaxi et al are analyzed, and improved scheme which satisfies properties of bid unforgeability, bid undeniability, bid confidentiality, bidder anonymity and collude attack resistance is presented, and the further research idea is given.

【Key words】sealed-bid auction; Hash function; Hash chain

1 概述

电子拍卖是电子商务的一项基本业务，是现实世界拍卖的电子化形式。密封式拍卖[1-5]要求每一个投标者的投标价格只能在关闭标价提交后才能打开投标，在开标阶段后，拍卖商公布获胜者和获胜价格。密封式拍卖应满足以下安全性需求：

(1)公平性：指所有投标者地位一样，不存在一方比其他方有更有利的条件。

(2)不可否认性：投标者投标后不能否认其投标。

(3)不可伪造性：投标者的投标不能被伪造。

(4)可证实性：可公开证明中标者标价的合法性。

(5)标价保密性：投标者的标价必须保密。

(6)时限性：确保投标结束后，才能打开投标。

(7)投标者匿名:投标参与者的身份(包括中标者的身份和未中标者的身份)必须保密。

目前用于电子拍卖的方法较多，如秘密共享、位承诺、Hash 函数、多方的秘密计算等[1-6]。其中，文献[4]提出基于 Hash 链的密封式电子拍卖方案，其最大的优点是能显著地降低投标和开标的时间。由于 Hash 函数从原理上讲也是单向函数，因此文献[5]提出更一般的基于单向函数的密封式电子拍卖方案。文献[6]提出一种新的基于 Hash 链的方案，该方案在不可否认性、不可伪造性、标价的保密性、时限性和抗合谋攻击等方面都存在安全问题。

2 Hash 链简介

密码学中的 Hash 函数是一个压缩函数，它将任意长度的消息压缩成固定长度的比特串，通常称为消息摘要、哈希值或数字指纹等。Hash 函数需要满足以下 3 个性质：

(1)抗原像(单向性)：找到任意一个消息使得其哈希值等于预先给定的值在计算上是不可行的。

(2)抗第二原像：找到任意第 2 个消息使其哈希值等于任意一个特定消息的哈希值在计算上是不可行的。

(3)抗碰撞：找到 2 个不同的消息使它们的哈希值相同在计算上是不可行的。

Hash 链是由一个公开的密码学 Hash 函数 h 进行递归运算得到的。随机选取一个种子值 s，令 $\omega_0=s$，在此基础上创建一条长为 n+1 的 Hash 链：

$\omega_i=h(\omega_{i-1})$, i=1, 2,…, n

在这里将 ω_n 称为 Hash 链的根节点。

3 文献[6]的方案及安全性分析

3.1 方案简介

一个拍卖包括 4 个实体：注册中心(registration center)，拍卖商(auctioneer)，卖主(vendor)和投标者(bidder)。其中，注册中心负责投标者参加投标注册；拍卖中心包括拍卖人和组织拍卖的人；卖主是想要卖商品的人；投标者为想得到商品的人。

(1)系统准备：拍卖商首先发布要拍卖的物品，并公布可接受的拍卖价 p_i (i=1, 2,…, m)，不妨设 $p_1>p_2>\cdots>p_m$，并且选

基金项目：国家“863”计划基金资助项目(2006AA01Z419)；国家自然科学基金重大研究计划基金资助项目(90604023)

作者简介：肖自碧(1974－)，女，讲师，主研方向：密码学，信息安全；杨 波，博士研究生；李寿贵，教授

收稿日期：2008-08-20 **E-mail：**holly_xzb@126.com

择一个散列函数 h 公布出去。

(2)注册：每个投标者 B_k(k=1, 2,…, t)到注册中心注册，注册中心检查每个投标者的身份和资格，如果合格就发放资格证书($cert_k$)。

(3)投标：首先每个投标者 B_k (k=1, 2,…, t)从 m 个公布的标价中选一个标价 $p_{k(i)}$，并随机选取一个数 $R_{k(i)}$，设 $\omega_{k(i)}^{(k)} = p_{k(i)} + h(R_{k(i)})$，在此基础上以相反的顺序创建一条如下式所示、长为 $k(i)$+1 的 Hash 链：

$$\omega_i^{(k)} = h(\omega_{i+1}^{(k)}) \quad (i = k(i)-1,\ k(i)-2,\cdots,\ 0)$$

B_k 传送给拍卖者的消息为 ($cert_k$, $h(R_{k(i)})$, $\omega_0^{(k)}$)，拍卖中心在一个合适的时间关闭标价提交。

(4)开标：拍卖商检查每个投标者 B_k 提交的消息，在 t 个消息中有 $h(p_1 + h(R_{k(i)})) = \omega_0^{(k)}$，说明 B_k 投了最高价 p_1，否则，说明无人投最高价 p_1，接着进行下一轮检查，如果在 t 个消息中有 $h^2(p_2 + h(R_{k(i)})) = \omega_0^{(k)}$，说明 B_k 投了最高价 p_2，否则，说明无人投最高价 p_2，按上述方法重复进行直到找到 t 个消息中有 $h^l(p_l + h(R_{k(i)})) = \omega_0^{(k)}$，说明 B_k 投了最高价 p_l。

(5)验证：最高价产生后，中标者提交随机数 $R_{k(i)}$，拍卖中心计算 $h^l(p_l + h(R_{k(i)})) = \omega_0^{(k)}$ 是否成立，如果成立则说明中标者确实投了最高价，否则，说明没有投最高价。其他投标者可通过计算提交的 $R_{k(i)}$来验证中标者的合法性。

3.2 安全性分析

在投标过程中，投标者 B_k 传送给拍卖商的消息为 ($cert_k$, $h(R_{k(i)})$, $\omega_0^{(k)}$)，由于投标者的资格证书 $cert_k$ 与他所承诺的 $h(R_{k(i)}), \omega_0^{(k)}$ 没有任何内在的联系，因此存在 2 种情形的伪造：(1)捣乱者或作弊者截获此消息，并按如下方式进行篡改：首先任意选择一个新的价格 $p_{k'(i)}$ 和一个随机数 $R_{k'(i)}$，然后按投标过程创建一条长度为 $k'(i)$+1 的 Hash 链，得到新的 $\omega_0'^{(k)}$，最后将消息 ($cert_k$, $h(R_{k'(i)})$, $\omega_0'^{(k)}$) 传送给拍卖者；(2)拍卖商自己由于某种目的类似与情况(1)篡改投标者 B_k 传送来的消息。因此，该方案不满足不可伪造性，从而也不能提供抗否认性。

此方案的一大优点是不需要交互，可在较大程度上减少通信量，但最大的缺点是在投标阶段就能打开投标，不具有时限性。当拍卖商接收到投标者 B_k 传来的消息 ($cert_k$, $h(R_{k(i)})$, $\omega_0^{(k)}$) 后，拍卖商可以从价格 p_1 开始进行穷举。若有 $h(p_1 + h(R_{k(i)})) = \omega_0^{(k)}$，说明 B_k 投了价 p_1，否则，接着进行下一轮检查，如有 $h^2(p_2 + h(R_{k(i)})) = \omega_0^{(k)}$，说明 B_k 投了价 p_2，否则，按上述方法重复进行直到找到有 $h^l(p_l + h(R_{k(i)})) = \omega_0^{(k)}$，说明 B_k 投了价 p_l。由于拍卖商可以在关闭标价提交前计算出所有的标价，因此拍卖商可以和某个投标者合谋进行有利于该投标者的投标。更为严重的是，如果某个投标者在关闭标价提交前截获所有的标价提交消息，他自己能和拍卖商一样计算出所有的投标价格，因此，无须合谋他就能提交一个有利于自己的投标价格。

显然，在投标阶段，任何的投标者均能根据投标算出所有的投标价格。因此，此方案不具备标价的匿名性。

4 改进方案及安全性分析

4.1 改进方案

本文将改进的方案称为双承诺方案，承诺一个随机数和承诺一个投标价格。

(1)系统准备

拍卖商首先发布要拍卖的物品，并公布可接受的拍卖价 p_i(i=1, 2,…, m)，不妨设 $p_1 > p_2 > \cdots > p_m$，并且选择一个散列函数 h 公布出去。

(2)注册

每个投标者 B_k(k=1, 2,…, t)到注册中心注册(注册中心作为可信第三方提供匿名性服务)，注册中心检查每个投标者的身份和资格，如果合格就发放资格证书 $cert_k$=(ID_k, $Pub\text{-}B_k$, $Sign\{ID_k, Pub\text{-}B_k\}_{Pri\text{-}TP}$)，其中，$ID_k$ 为投标者 B_k 的临时身份；$Pub\text{-}B_k$ 为 B_k 的临时公钥；$Pri\text{-}TP$ 为注册中心的私钥；符号 $Sign\{M\}_{key}$ 表示用私钥 key 对消息 M 签名。注册中心安全传送给 B_k 临时的私钥 $Pri\text{-}B_k$。

(3)投标

每个投标者 B_k(k=1, 2,…, t)从 m 个公布的标价中选一个标价 $p_{k(i)}$，并选取一个随机数 $R_{k(i)}$，设 $\omega_{k(i)}^{(k)} = p_{k(i)} \| R_{k(i)}$，$\|$ 表示级联操作。在此基础上以相反的顺序创建一条长为 $k(i)$+1 的 Hash 链：$\omega_j^{(k)} = h(\omega_{j+1}^{(k)})$ ($j = k(i)-1,\ k(i)-2,\cdots,\ 0$)

B_k 传送给拍卖商的消息为 ($cert_k$, $h(R_{k(i)})$, $\omega_0^{(k)}$, $Sign\{h(R_{k(i)}), \omega_0^{(k)}\}_{Pri\text{-}B_k}$)，拍卖中心在一个合适的时间关闭标价提交。

(4)开标

每个投标者 B_k 向拍卖商提交消息 $R_{k(i)}$。拍卖商先通过计算 $h(R_{k(i)})$验证 $R_{k(i)}$的真实性，然后检查每个投标者 B_k 提交的消息，若在 t 个消息中有 $h(p_1 \| R_{k(i)}) = \omega_0^{(k)}$，则说明 B_k 投了最高价 p_1，否则，说明无人投最高价 p_1，接着进行下一轮检查，如果在 t 个消息中有 $h^2(p_2 \| R_{k(i)}) = \omega_0^{(k)}$，说明 B_k 投了最高价 p_2，否则，说明无人投最高价 p_2，按上述方法重复进行直到找到 t 个消息中有 $h^l(p_l \| R_{k(i)}) = \omega_0^{(k)}$，说明 B_k 投了最高价 p_l。

4.2 安全性分析

改进的方案具有不可否认性、不可伪造性、时限性和投标者匿名、可验证性和抗合谋攻击等性质。

(1)不可否认性。新方案基于双承诺。首先，B_k 传送给拍卖商消息 ($cert_k$, $h(R_{k(i)})$, $\omega_0^{(k)}$, $Sign\{h(R_{k(i)}), \omega_0^{(k)}\}_{Pri\text{-}B_k}$)，$B_k$ 通过签名向拍卖商保证了标价信息 $\omega_0^{(k)}$ 的真实性，实质上是对自己的标价进行了一个承诺；其次，因为 Hash 函数具有抗碰撞、抗第二原象和抗原象的性质，实质上 $Sign\{h(R_{k(i)}), \omega_0^{(k)}\}_{Pri\text{-}B_k}$，$h(R_{k(i)})$，$R_{k(i)}$形成了承诺链，由 $Sign\{h(R_{k(i)}), \omega_0^{(k)}\}_{Pri\text{-}B_k}$ 保证了 $h(R_{k(i)})$是投标者 B_k 产生的，由 $h(R_{k(i)})$保证了 $R_{k(i)}$只有 B_k 才知道。拍卖商可以通过 $cert_k$ 里的公钥验证签名，并在开标时通过 $h(R_{k(i)})$来验证 $R_{k(i)}$的真实性。这就保证了不可否认性。

(2)不可伪造性。由于投标信息有投标者 B_k 的数字签名，因此 B_k 的投标是不能被伪造的。此外，投标者自己不能伪造一个新的 $p_{k'(i)}$ 使得 $h^{k'(i)}(p_{k'(i)} \| R_{k(i)}) = \omega_0^{(k)}$。因为，如果出现这种情况，则找到了 Hash 函数的碰撞。

(3)时限性和投标者匿名。由于新方案须在开标后进行一次通信才能揭示投标者的标价，保证了时限性。由于引入了提供匿名服务的可信第 3 方，只要可信第 3 方不与拍卖方合谋就能够实现投标者的匿名性。

(4)可验证性和抗合谋攻击。由于投标者的 $R_{k(i)}$是发布的，任何人都可以证明投标者中标、未中标者被淘汰的正确性。新方案具有时限性，能防止合谋攻击。 (下转第 168 页)