何大可 黄月江 编

密码学进展

——ChinaCrypt'2007

中国密码学会2007年会论文集

西南交通大学出版社
Http://press.swjtu.edu.cn

内 容 简 介

本书是2007年10月在成都召开的中国密码学会2007年会论文集。书中收录了涉及密码学若干分支的研究论文54篇。主要内容包括：序列密码与分组密码、公钥密码、Hash函数与数字签名、密码协议、量子密码、密码实现与应用等。

本书可供从事密码学、信息安全、通信与信息系统、计算机应用技术等专业的科技人员和高等院校师生参考。

图书在版编目（CIP）数据

密码学进展：中国密码学会2007年会论文集 / 何大可，黄月江编. —成都：西南交通大学出版社，2007.10
ISBN 978-7-81104-742-4

Ⅰ. 密… Ⅱ. ①何…②黄… Ⅲ. 密码 — 理论 — 文集
Ⅳ. TN918.1-53

中国版本图书馆CIP数据核字（2007）第152334号

密码学进展——中国密码学会2007年会论文集

何大可 黄月江 编

*

责任编辑 万 方
特邀编辑 于 河
封面设计 本格设计
西南交通大学出版社出版发行
（成都二环路北一段111号 邮政编码：610031 发行部电话：028-87600564）
http://press.swjtu.edu.cn
E-mail: cbsxx@swjtu.edu.cn
四川森林印务有限责任公司印刷
*
成品尺寸：185 mm × 260 mm 印张：22.75
字数：655千字
2007年10月第1版 2007年10月第1次印刷
ISBN 978-7-81104-742-4
定价：88.00元

中国密码学会2007年会程序委员会

主　席：何大可（西南交通大学）

副主席：黄月江（中国电子科技集团公司第三十研究所）

委　员：（按姓氏笔画及汉语拼音排序）

马建峰（西安电子科技大学）
王小云（山东大学）
冯克勤（清华大学）
冯登国（中国科学院软件所）
刘木兰（中国科学院数学与系统科学研究院）
朱　洪（复旦大学）
李　宝（中国科学院研究生院）
李　祥（贵州大学）
杨义先（北京邮电大学）
杨伟成（中国船舶重工集团公司第七二二研究所）
张焕国（武汉大学）
秦志光（电子科技大学）
徐茂智（北京大学）
曹珍富（上海交通大学）
符方伟（南开大学）
彭国华（四川大学）
裴定一（广州大学）

序　言

由中国密码学会主办、西南交通大学承办的中国密码学会 2007 年会（China Crypt'2007）于 2007 年 10 月 19 日至 22 日在中国成都西南交通大学召开。

本次年会共收到投稿论文 116 篇，每篇论文至少由两位专家评审。程序委员会认真讨论了评审结果，并且征询拟录用论文作者本人意见，最后确定录用论文 54 篇，其中 37 篇为全文录用，17 篇为短文录用。

本论文集收录的这 54 篇论文，内容涉及序列密码与分组密码、公钥密码、Hash 函数与数字签名、密码协议、量子密码、密码实现与应用等研究方向。这些论文部分地反映了我国密码学学术界当前的研究动态和学术水平。

本次年会，无意间创造了 3 个月征文、3 个月论文成集的新记录。为此，我们首先要感谢所有向本次年会投稿的作者，感谢他们对本次年会征文的迅速响应，这是对中国密码学会及本次年会最大的支持。其次，要感谢所有参与稿件评审的专家，他们为了从众多的稿件中遴选出最具代表性的论文参加年会交流付出了辛勤的劳动。我们还要感谢西南交通大学信息安全与国家计算网格实验室的老师和研究生们以及西南交通大学出版社，没有他们的帮助，不可能在如此短的时间内完成论文集的稿件处理、编辑校对和印刷出版。

本次年会和论文集的出版得到中国密码学会和学会主管单位的大力支持，在此一并致谢！

中国密码学会 2007 年会程序委员会

2007 年 10 月

目 录

序列密码与分组密码

公钥密码

杂凑函数与数字签名

密码协议

量子密码

密码实现与应用

短 文

附 件

Remarks on Receipt-free Auction/Voting Schemes Using Commitment*

Chunhui Wu[1] Xiaofeng Chen Fangguo Zhang[1] Hyunrok Lee[2] Kwangjo Kim[2]

[1]School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275, P.R.China

[2]Information and Communications University (ICU), Taejon 305-714, KOREA

chunhuiwu@163.com, {isschxf, isszhfg}@mail.sysu.edu.cn, {tank, kkj}@icu.ac.kr

Abstract: In this paper, we point out some weaknesses of the receipt-free auction and voting schemes using trapdoor commitment [1, 2]. We can prove even if only one auctioneer (or tally authority) is dishonest, the receipt-freeness of these schemes can not be achieved.

Key words: Electronic auction; Electronic voting; Receipt-freeness; Trapdoor commitment

1 Introduction

Abe and Suzuki [1] proposed the first receipt-free sealed-bid auction scheme with the idea of making trapdoor commitment on the bidding price. Okamoto [2] proposed two improved receipt-free voting schemes using blind signatures and trapdoor commitment. These schemes seem to be receipt-free since the bidders (or voters) can open the commitment in any way with the trapdoor information. However, we argue that the use of trapdoor commitments in these two schemes is insufficient to achieve receipt-freeness. The main idea is that the coercer can compute the trapdoor information of the winning bidder (or voter), *i.e.*, the secret key as a receipt, which is equivalent to solve the Discrete Logarithm Problem (DLP) in the group with large prime order.

2 Cryptanalysis of Abe–Suzuki's Auction Scheme

In the Abe-Suzuki's auction scheme [1], the sequence of commitments $(C_{1,j}, C_{2,j}, \cdots, C_{m,j})$ of each bidder B_j is published for public verification. So, the coercer also knows the victim's commitments. In the opening phase, note that each auctioneer A_i publishes shares $r_{l,j}^{i}$ $(j = 1,2,\cdots,b)$ of i-th secret seeds $r_{l,j}$ of all bidders B_j. All auctioneers then recover secret seeds $r_{l,j}$ and check the following equalities $C_{l,j} = g^{M_l} h_j^{r_{l,j}}$ $(j = 1,2,\cdots,b)$ for all

* Supported by National Natural Science Foundation of China (No.60503006) and NSFC-KOSEF Joint Research Project (No. 60611140543).

bidders B_j. Therefore, all auctioneers (including the dishonest auctioneer who colludes with the coercer) know the winner's secret seeds and the corresponding commitment. Without loss of generality, we denote the winner is B_w and the winning price $p_{win} = p$. The dishonest auctioneer then sends the winner's secret seeds $r_{p,w}$ and the corresponding commitment $C_{p,w}$ to the coercer. If $C_{p,w}$ belongs to a victim, the coercer then orders the victim to open the commitment $C_{p,w}$. Since the victim knows the trapdoor information x_w, he can open the commitment freely, *i.e.*, he can show the pair (M_0, r^*) such that $M_0 + x_w r^* = M_1 + x_w r_{p,w}$. However, the coercer can compute the trapdoor information (*i.e.*, secret key) $x_w = (M_0 - M_1) \cdot (r_{p,w} - r^*)^{-1}$ as a receipt.

3 Cryptanalysis of Okamoto's Voting Scheme

In Okamoto's improved voting scheme [2], V_i must know the trapdoor information α_i to provide a zero-knowledge proof in the voting booth, which means that he can open the commitment in any desired ways. However, we argue that the scheme is still not receipt-free if T colludes with the coercer. Since the voter must know the trapdoor information α_i, it is meaningless for the coercer to control α_i. We assume that the voter can choose his/her secret key α_i freely. At the end of the claiming stage, the coercer requires the victim V_i to reveal his/her commitment $(m_i \| G_i, s_i)$ and the corresponding vote information (v_i^*, r_i^*). Only if the commitment $(m_i \| G_i, s_i)$ is on the bulletin board and $m_i = g^{v_i^*} G_i^{r_i^*} \bmod p$, the coercer accepts them. The coercer then colludes with T and knows the vote information (v_i, r_i) related with m_i. If $(v_i^*, r_i^*) = (v_i, r_i)$, the coercer believes the voter V_i obeys the rules. Otherwise, he punishes the voter V_i and shows the trapdoor information $\alpha_i = (v_i^* - v_i) \cdot (r_i - r_i^*)^{-1}$ as a receipt.

4 Conclusion

In this paper, we point out some weaknesses of the receipt-free auction and voting schemes using trapdoor commitment [1, 2]. Therefore, it must be careful to design receipt-free auction and voting schemes using the key-exposure trapdoor commitment schemes.

References

[1] M. Abe and K. Suzuki, *Receipt-Free Sealed-Bid Auction*, ISC 2002, LNCS 2433, pp.191-199, Springer-Verlag, 2002

[2] T. Okamoto, *Receipt-free electronic voting schemes for large scale elections*, Proceeding of Workshop on Security Protocols 1997, LNCS 1361, pp.25-35, Springer-Verlag, 1997

关于使用承诺方案的无收据的拍卖/投票方案的注记

伍春晖[1] 陈晓峰[1] 张方国[1] Hyunrok Lee[2] Kwangjo Kim[2]

[1]中山大学信息科学与技术学院 广州 510275 中国

[2]信息与通信大学 大田 305-714 韩国

摘 要：本文我们给出了一些基于陷门承诺的无收据的拍卖/投票方案的缺陷。我们证明即使只有一个拍卖行（计票机构）是不诚实的，那么这些方案也没有无收据性。

关键词：电子拍卖 电子投票 无收据性 陷门承诺

责任编辑 / 万 方
特邀编辑 / 于 河
封面设计 / Design 本格设计

密码学进展
——ChinaCrypt'2007
中国密码学会2007年会论文集

ISBN 978-7-81104-742-4
9 787811 047424 >
定价：88.00元