电子与信息学报 2005 27 (4): 608-611 ISSN: 1009-5896 CN: 11-4494/TN

论文

可公开验证的ElGamal / RSA加密

伍前红, 王继林, 袁素春, 王育民

西安电子科技大学ISN国家重点实验室119信箱 西安 710071

收稿日期 2003-12-25 修回日期 2004-6-15 网络版发布日期 2008-4-14 接受日期

摘要
可公开验证加密允许任何实体验证加密的消息和先前承诺的秘密一样，但不会泄漏明文的任何信息。这在公平交换、防欺骗的秘密分享和安全多方计算中有重要应用。该文分别给出可公开验证的ElGamal加密和RSA加密方案。其中前者是Stalderr方案的改进，改进后的方案是语义安全的而Stalder方案达不到语义安全性。同时将该方案推广到了多个接受者的情形，最后给出了高效的可公开验证RSA加密方案。

关键词 可公开验证加密 零知识证明 bit承诺 RSA体制 ElGamal体制

分类号 TN918

Publicly Verifiable Encryption for ElGamal/RSA Encryption

Wu Qian-hong, Wang Ji-lin,Yuan Su-chun,Wang Yu-min

Stte Key Lab.of Integrated Service Networks. Xidian Univ.,Xi ’ an 110071 China

Abstract
A publicly verifiable encryption scheme allows any entity to verify that a cipher-text hides the same message as committed before without revealing it. It is important to construct fair exchange scheme, publicly verifiable secret sharing and cheater-resistant secure multi-party computation. In this paper, publicly verifiable encryption schemes are presented for ElGamal/RSA cryptosystem. The ElGamal case is an improved version of Stadler publicly verifiable encryption scheme. The improved scheme is semantic secure while Stadler scheme is not. Also, the scheme is extended to the context of multi-recipient ElGamal encryption and an efficient publicly verifiable RSA scheme is proposed.

Key words Publicly verifiable encryption （PVE） Zero-knowledge Proof of Knowledge （ZPK） Bits commitment RSA cryptosystem ElGamal cryptosystem

DOI:

通讯作者

作者个人主页 伍前红; 王继林; 袁素春; 王育民