通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

李龙海,付少锋,苏锐丹.基于双线性对的乐观Mix-net协议[J].通信学报,2013,(11):153~161

基于双线性对的乐观Mix-net协议

Optimistic Mix-net protocol based on bilinear pairings

投稿时间： 2012-11-01

DOI：10.3969/j.issn.1000-436x.2013.11.017

中文关键词：匿名通信 乐观混合网络 双线性对 秘密混洗证明

英文关键词:anonymous communication optimistic mix network bilinear pairings proof of secret shuffling

基金项目:国家自然科学基金资助项目(61101142)；中央高校基本科研基金资助项目(K50510030012)

作者	单位
李龙海，付少锋，苏锐丹	西安电子科技大学 计算机学院，陕西 西安 710071

中文摘要:

提出了一种新的基于双线性对的乐观Mix-net协议。利用双线性对工具简化了密钥管理，在不同的协议会话中服务器端不用重新生成密钥，并且当前会话不会为其他会话提供解密预言机服务。采用了“哑元追踪法”保证混洗过程的完整性，简化了正确性证明的构造。对ElGamal联合解密过程做了优化，降低了每个服务器节的指数运算量。在没有服务器作弊的情况下，对输入密文组的混洗和解密速度比其他可公开验证的Mix-net方案高得多。

英文摘要:

A novel pairing-based optimistic Mix-net scheme was proposed. The key management is made easier by employing bilinear paring primitives and there is no need for the participating mix servers to re-generate keys jointly between mix-sessions to avoid providing decryption oracle service to other mix-sessions. Integrity of messages during mixing is partially guaranteed by using “dummy messages tracing” technology resulting in a simpler construction for proofs of correctness. An optimization method for the joint ElGamal decryption involved in the protocol was also proposed, which can reduce the number of exponentiations computed by each mix server. The Mix-net will shuffle and decrypt input ciphertexts much faster than all previous Mix-nets with public verifiability when all mix servers execute the mixing protocol honestly.

查看全文 查看/发表评论 下载PDF阅读器

关闭