计算机工程与应用 2008 44 (19): 109-111 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于ECC组合公钥的GSM双向认证

张 毅[2], 崔天喜[1,2], 唐 红[1,2]
1.重庆邮电大学 计算机学院，重庆 400065
2.重庆邮电大学 移动通信技术重点实验室，重庆 400065

收稿日期 2007-12-20 修回日期 2008-3-6 网络版发布日期 2008-6-26 接受日期

摘要 针对目前GSM网络认证和密钥协商过程中存在的安全隐患，提出了基于椭圆曲线组合公钥技术的GSM离线双向认证，在引入了非对称密钥加密的同时却不需要引入可信任第三方CA机构，能有效解决大规模网络环境中密钥生产、分发、存储管理与证书验证难等问题。实验分析表明，该方案不仅实现了GSM的双向认证，而且与其它方案相比，节省了网络带宽，降低了对存储空间的要求，且每次认证都实现了加密密钥刷新。

关键词 GSM双向身份认证 CPK标识认证 密钥协商协议
分类号

Mutual authentication in GSM based on Elliptic Curve Cryptography and combined public key technology

ZHANG Yi[2],CUI Tian-xi[1,2],TANG Hong[1,2]

1.College of Computer Science，Chongqing University of Posts and Telecommunication，Chongqing 400065，China
2.Lab. of Mobile Telecommunication Technology，Chongqing University of Posts and Telecommunication，Chongqing 400065，China

Abstract
In this paper an improvement to the GSM authentication protocol is proposed，which is the off-line mutual authentication of GSM based on Elliptic Curve Cryptography and Combined Public Key（CPK） technology.The proposed protocol utilizes asymmetric key cryptography in no need of setting up the third certificate agent，be able to resolve the problems in the production distribution and management of the key and the validation of the certificates in great network environment.The proposed protocol provides mutual authentication，requires less storage，avoids replay attack，consumes smaller network bandwidth，be capable of stream key’s updating every time.

Key words mutual authentication for GSM identity authentication based on CPK key agreement protocol

DOI:

通讯作者 张 毅 letianfly@sohu.com