计算机工程与应用 2007 43 (20): 128-131 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

基于椭圆曲线自验证公钥的3G通信认证方案

黄 亮，卢建朱

广州暨南大学 计算机科学系，广州 510630

收稿日期 修回日期 网络版发布日期 2007-6-29 接受日期

摘要 采用将PKBP（公钥广播协议）和SPAKA（基于自验证公钥的认证及密钥交换协议）相结合的方法，基于椭圆曲线上的离散对数难问题，设计了一种3G通信中的双向认证和密钥协商的认证系统，其安全性是基于椭圆曲线上的离散对数难问题的。与现有公钥认证协议相比，PKBP和SPAKA减少了数据传输量的和VLR与ME的在线计算量，可在无须传送公钥证书的前提下完成ME和VLR的相互认证及会话密钥协商，并可在特定场合实现对ME通话的可控、合法监听。因此，该方案提高了认证系统的安全性和效率，很适合于支持3G系统的全球移动性和通信安全性。

关键词 3G安全 身份认证 自验证公钥 协议分析

分类号

Authentication scheme with self-certified public-key in 3G

HUANG Liang，LU Jian-zhu

Computer Science Department，Jinan University，Guangzhou 510630，China

Abstract

Based on the elliptic curve discrete logarithm problem，we adopt approaches to combining PKBP（Public-Key Broadcast Protocol）with SPAKA（Self-certified Public-key based Authentication and Key Agreement Protocol），and then design a mutual authentication and key agreement authentication system used in 3G communications.Its security is based on the elliptic curve discrete logarithm problem.Compared with other public-key based authentication protocols，SPAKA associated with PKBP reduces communicational payloads and Mobile Equipment（ME） can enforce mutual authentication with VLR without delivering its public-key certificate to VLR.Besides，the conversation launched by ME can be monitored in a controllable and legitimate way at required occasions.Thus this scheme that improves the security and efficiency of authentication system is well suited for supporting globe mobility with low computational loads and secure communication.

Key words 3G security identity authentication self-certified public-key protocol analysis

DOI:

通讯作者 黄 亮 E-mail：itcshl@163.com