计算机工程与应用 2007 43 (24): 123-124 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

对一个数字签名方案安全性证明的注记

齐亚平[1]，刘文化[2]，禹 勇[3]

1.西安航空技术高等专科学校 计算机系，西安 710077
2.济源职业技术学校 计算机系，河南 济源 454650
3.西安电子科技大学 ISN国家重点实验室，西安 710071

收稿日期 修回日期 网络版发布日期 2007-8-9 接受日期

摘要 研究了Willy，Zhang和Yi等学者提出的基于身份的强指定验证者签名方案（简记为WZY方案）的安全性证明，发现在他们的安全性证明中存在漏洞：在证明签名方案的不可伪造性时，敌手拥有指定验证者的私钥。在一个简单的假设下：假设对于一个有效的输入，Hash函数的输出是随机的，并且敌手事先知道这个输入，重新证明了WZY方案的不可伪造性依赖于双线性Diffie-Hellman问题，从而完善了WZY方案的安全性证明。

关键词 数字签名 强指定验证者签名 双线性对

分类号

Notes onsecurity proof of digital signature scheme

QI Ya-ping[1]，LIU Wen-hua[2]，YU Yong[3]

1.Department of Computer，Xi’an Aerotechnical College，Xi’an 710077，China
2.Department of Computer，Jiyuan Vocational and Technology College，Jiyuan，Henan 510642，China
3.National Key Lab of ISN，Xidian University，Xi’an 710071，China

Abstract

Recently，Willy、Zhang and Yi proposed an identity-based strong designated verifier signature scheme（noted as WZY scheme） and gave the security proof of the scheme.Unfortunately，We find that their security proof is improper：in the proof of the unforgeability of the scheme，they supposed that the adversary has the secret key of the designated verifier.Under a simple assumption that the hash function is considered as an oracle that on each valid input known to the adversary beforehand produces a random value，a new proof that the unforgeability of WZY scheme relies on the Bilinear Diffie-Hellman Problem is given.

Key words digital signature strong designated verifier signature bilinear pairings

DOI:

通讯作者 齐亚平 E-mail：qiyaping2006@21cn.com