计算机工程与应用 2009 45 (12): 8-11 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

常数大小自主可链接的门限环签名

王 薇, 魏普文, 王明强, 张立江

山东大学 密码技术与信息安全教育部重点实验室，济南 250100

收稿日期 2008-12-30 修回日期 2009-2-2 网络版发布日期 2009-4-20 接受日期

摘要 进一步分析讨论Shacham和Waters提出的环签名方案的潜在性质，提出相应的门限环签名方案。与Wei和Yuen的方案相比，在无随机谕示模型下，该门限环签名方案的安全性证明基于标准假设——计算Diffie Hellman假设与子群判定假设。此外，在某些情况下，该方案可以转化为常数大小自主可链接的门限环签名，从而提高签名效率。

关键词 门限环签名 可链接 随机谕示 标准假设

分类号

Constant-size self linkable threshold ring signatures

WANG Wei,WEI Pu-wen,WANG Ming-qiang,ZHANG Li-jiang

Key Laboratory of Cryptographic Technology and Information Security，Ministry of Education，Shandong University，Jinan 250100，China

Abstract

A further discussion on the potential properties of Shacham and Waters ring signatures is made and the corresponding threshold ring signature schemes are presented.Compared with the schemes without random oracle proposed by Wei and Yuen，the threshold ring signature is provable secure under standard assumptions（CDH and SGH）.Besides，in order to improve the efficiency of the signature in some cases，the schemes can be converted to a constant-size self linkable threshold ring signature.

Key words threshold ring signature linkable random oracle standard assumptions

DOI: 10.3778/j.issn.1002-8331.2009.12.003

通讯作者 王 薇 weipuwen@mail.sdu.edu.cn