格上后向无关联性安全的验证者本地撤销群签名

张彦华[1]，刘西蒙[2]，胡予濮[3]，甘勇[4]，贾惠文[5]
[1]郑州轻工业大学计算机与通信工程学院，中国郑州市，450001
[2]福州大学数学与计算机科学学院，中国福州市，350108
[3]西安电子科技大学综合业务网理论及关键技术国家重点实验室，中国西安市，710071
[4]郑州工程技术学院信息工程学院，中国郑州市，450044
[5]广州大学数学与信息科学学院，中国广州市，510006

摘要：群成员可撤销的群签名中，验证者本地撤销机制似乎是一种更为灵活的选择，因为在签名验证过程中，仅需验证者获取最新的撤销信息，而不涉及签名者。与经典的数论型构造相对应，Langlois等人给出了后量子安全的首个格上验证者本地撤销群签名。然而，截至目前，所有格上验证者本地撤销群签名方案暂不满足后向无关联性，该特性可保障群成员被撤销前其对消息签名的匿名性和无关联性。本文给出了首个格上后向无关联性安全的验证者本地撤销群签名方案，从而解决了这一公开问题。新方案为群公钥和群成员签名密钥节省了$O(\log N)$的比特大小，并且没有任何公钥加密。特别地，新方案在随机谕言机模型下是可证明安全的，其困难性可归约至两个经典格上难题假设，即小整数解难题和差错学习难题。

关键词：群签名；格密码；验证者本地撤销；后向无关联性；小整数解难题
https://doi.org/10.1631/FITEE.2000507