无随机预言模型的盲签名

http://www.firstlight.cn 2010-05-01

近些年来，盲签名的研究取得了很多的成果，但也存在着计算过程复杂、传输效率低、交互次数频繁等问题。基于Boneh等人提出的签名，首先给出一个不包含随机预言模型的盲签名方案。不包括随机预言机，盲签名就是一个可实现的安全的标准方案，而考虑到交互次数问题，该方案还可以引入公共参考串(common reference string, CRS)来完成签名方的非交互零知识证明，使得盲签名算法仅包含两次交互，实现了轮优先round optimal，在此基础上也可以实现盲签名算法的并发执行。该盲签名算法构造简单且计算复杂度较低，因此比现有的盲签名方案更加有效，节省了传输带宽，提高了传输效率。

存档文本