基于XTR体制的盲签名方案的改进

http://www.firstlight.cn 2008-05-18

分析陈晓峰、高虎明和王育民提出两种基于XTR体制的盲签名方案，即XTR-Blind-Nyberg-Rueppel和XTR-Blind-Schnorr签名方案，通过对XTR密钥恢复算法中的“最小者”条件进行充分考虑，分别改进这两种盲签名方案。在同等安全程度下，改进方案所交换的数据量分别约为原Blind-Nyberg-Rueppel和Blind-Schnorr签名方案的1/3，并且改进方案的计算速度大大提高。

存档文本