基于Hess签名的公开可验证签密方案

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

利用Hess基于身份的数字签名方案，提出了一个基于身份的公开可验证加密签名方案。在BDH问题是困难的假设下，运用随机预言模型证明了该方案的安全性。方案在拥有基于身份密码体制独特优点的同时，又能保证在不访问明文的情况下，任何第三方都可以认证密文。证明了方案具有前向安全性，即使签名者的私钥泄漏，第三方也不能恢复所签密消息的明文。新方案仅需2次双线性对运算，比目前效率最高的Chen和Malone-Lee方案少1次。

存档文本