基于ECC的病历文档内容抽取签名方案的研究

http://www.firstlight.cn 2010-07-01

针对当前电子病历交互信息的机密性、患者的隐私权及签名效率过低等问题，提出基于椭圆曲线密码体制（ECC）的内容抽取签名方案。该方案能从签名过XML病历文档中抽取指定部分，并能认证出抽取部分是由原始签名者签名，从而隐藏患者的隐私信息。实验结果表明，该方案整体实现效率较高，有较好的可操作性及可扩展性。

存档文本