隐式证书下的椭圆曲线数字签名算法的批认证方法

申请号：CN201910231811.5

专利号：ZL201910231811.5

专利名称：隐式证书下的椭圆曲线数字签名算法的批认证方法

专利申请时间：2019.7.05

专利授予时间：2020.3.31



## 摘要

本发明公开了一种隐式证书下的椭圆曲线数字签名算法的批认证方法，其主要方法为：判断“每个待认证数据的签名的第一个参数的和”是否等于“每个待认证数据的签名的第二个参数的逆与该待认证数据的摘要值的乘积之和与对应的椭圆曲线上的基点的乘积的结果”加上“每个待认证数据的签名的第二个参数的逆与签名的第一个参数的x坐标值、隐式证书的待签名部分的摘要值、数据发送方的公钥的重构因子的乘积之和”加上“每个待认证数据的签名的第二个参数的逆与签名的第一个参数的x坐标值的乘积之和与证书中心的公钥的乘积得到的结果”，若是则该批次的数据包均合法，通过认证，否则不通过认证。本发明提出的批认证方法能够明显提高系统吞吐率。

## 可能应用的场景

当用户接收到大量的签名的数据包后，典型的做法是，分别对每个数据包进行认证，然而这样的认证方法的开销很大。

而本发明提供的隐式证书下的椭圆曲线数字签名算法的批认证方法解决了用户通过多个匿名证书来保护数据时认证开销大的问题。

在用户需要验证CA颁发的多个匿名证书时使用该方法可以提高系统吞吐率。