

学院首页 > 区块链教程 > 新手入门 > 什么是椭圆曲线数字签名算法（ECDSA）？

# 什么是椭圆曲线数字签名算法（ECDSA）？

无主之地 副船长 船龄 7.7年

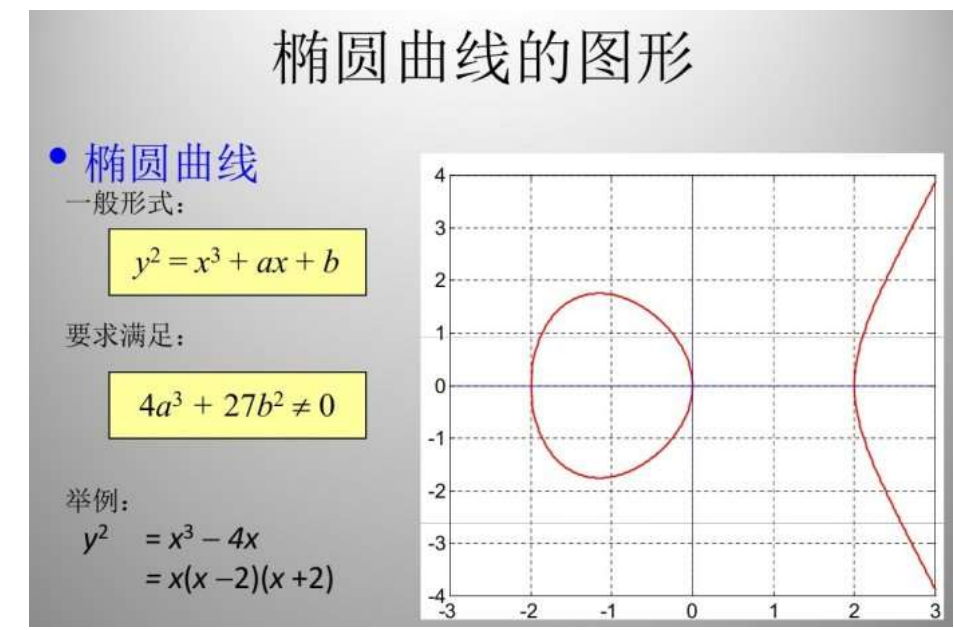
2013-10-01 02:01:00

来源

👁 89609

💬 0

椭圆曲线数字签名算法（ECDSA）是使用 **椭圆曲线密码（ECC）** 对数字签名算法（DSA）的模拟。ECDSA于1999年成为ANSI标准，并于2000年成为IEEE和NIST标准。它在1998年既已为ISO所接受，并且包含它的其他一些标准亦在ISO的考虑之中。与普通的离散对数问题（discrete logarithm problem DLP）和大数分解问题（integer factorization problem IFP）不同，椭圆曲线离散对数问题（elliptic curve discrete logarithm problem ECDLP）没有亚指数时间的解决方法。因此椭圆曲线密码的单位比特强度要高于其他公钥体制。






数字签名算法（DSA）在联邦信息处理标准FIPS中有详细论述，称为数字签名标准。它的安全性基于素域上的离散对数问题。椭圆曲线密码（ECC）由Neal Koblitz和Victor Miller于1985年发明。它可以看作是椭圆曲线对先前基于离散对数问题（DLP）的密码系统的模拟，只是群元素由素域中的元素数换为有限域上的椭圆曲线上的点。椭圆曲线密码体制的安全性基于椭圆曲线离散对数问题（ECDLP）的难解性。椭圆曲线离散对数问题远难于离散对数问题，椭圆曲线密码系统的单位比特强度要远高于传统的离散对数系统。因此在使用较短的密钥的情况下，ECC可以达到与DL系统相同的安全级别。这带来的好处就是计算参数更小，密钥更短，运算速度更快，签名也更加短小。因此椭圆曲线密码尤其适用于处理能力、存储空间、带宽及功耗受限的场合。

ECDSA是椭圆曲线对DSA的模拟。ECDSA首先由Scott和Vanstone在1992年为了响应NIST对数字签名标准（DS S）的要求而提出。ECDSA于1998年作为ISO标准被采纳，在1999年作为ANSI标准被采纳，并于2000年成为IEEE和FIPS标准。包含它的其他一些标准亦在ISO的考虑之中。

全部 最佳

登录 账号发表你的看法，还没有账号？立即免费 注册





巴比特学院是巴比特旗下的教育培训品牌，由巴比特主办，与专业培训机构合作，邀请业内区块链专家和实践者作为培训导师，通过导师现场授课、行业高端论坛、企业调研走访等方式，打造国内一流区块链培训品牌，推动区块链在中国的发展与创新。2018年，巴比特学院的品牌影响力将向杭州以外的北京、上海、南京、成都、深圳、广州等地辐射。

关于我们

关于巴比特

使用条款

版权声明

品牌素材

联系我们

联系人：学院课代表

微信：btczs001

地址：杭州市西湖区西溪首座

扫码咨询

