① 风险提示: 防范以"虚拟货币""区块链"名义进行非法集资的风险 —银保监会等五部门

Q

资讯 ▼

快讯

视频 ~

产业区块链

学院 ▼

海盗号

更多 画市日

搜索...

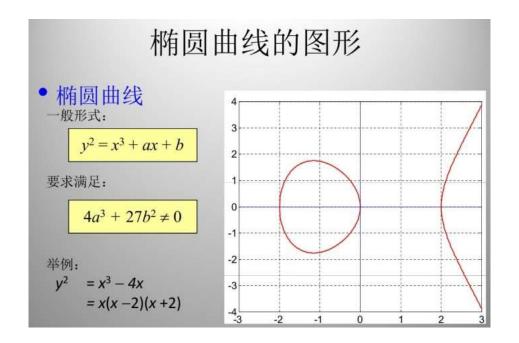
⑥ 学院首页 > 区块链教程 > 新手入门 > 什么是椭圆曲线数字签名算法 (ECDSA) ?

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<mark>椭圆曲线密码(ECC</mark>) 对数字签名算法(DSA)的模拟。ECDSA于19 99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(inte ger 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可以达到于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IEE E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

凸点赞0

☆2次收藏 ペ分享 下一篇: 比特币交易所Tradehill将要拍卖挖矿...

推荐教程

加密的钱包如何获得POS利息?

小编之前曾撰写了教程,详细介绍了什么是 息,如果您还不清楚什么是POS,请点击

Bytom PHP SDK 使用指南

工作量证明机制是怎样的?

比特币地址为什么不会输错?

比特币区块链的数据结构解析

比特币有哪些本地或在线钱包?

比太钱包为什么从 Bitcoinj 切换到了

Scrypt 算法虚拟币挖矿教程

如何解释以太坊是什么?

点点币完全节点的介绍和设置





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



Copyright © 2011-2020 · 巴比特 · 署名-非商业性使用-相同方式共享(BY-NC-SA 3.0 CN) · 浙ICP备14013035号-8 · 學 浙公网安备 33010602002085号 · 站长统计 · 文章存档

