

抗量子签名服务

词汇表

产品文档



腾讯云

【 版权声明 】

©2013–2022 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

词汇表

最近更新时间：2022-01-18 16:16:59

抗量子签名

可以抵抗量子计算机破解的数字签名，同时也可以抵抗传统计算的攻击。抗量子签名相比传统的数字签名有更好的安全性。

量子计算机

基于量子力学原理的计算设备，使用量子比特进行数据存储和量子算法进行数据操作。量子计算机相比传统计算机，在部分问题上拥有更高的运算效率，例如搜索、因数分解等。量子计算机可以破解当前主流的非对称加密算法，是目前密码学安全的一个已知威胁。

数字签名

对数据信息进行鉴别的一种方法，可以对原始数据进行完整性验证和不可抵赖性验证。传统的数据签名方案大多使用非对称加密算法来实现，存在被量子计算机破解的风险。

真随机熵源

基于量子物理原理的真随机数发生器，生成完全不可预测的随机数。相比基于算法来保证安全的传统密码学随机数发生器，具有更高的安全性。