**安全等级**

密码学的安全等级可用于指导系统设计时密码学协议的参数选取，如

密钥长度的选取。经常提到的安全等级有 80-bit，128-bit，256-bit

等。分别意味着目前**已知的最快攻击算法**攻破相应的密码学协议需要

2 28，2 128，2 256量级的尝试次数。

根据欧盟支持的研究机构 ECRYPT-CSA 的推荐，目前的新系统不应该

再使用 80-bit 的安全等级。128-bit 的安全等级可以保证 10 年的安

全性。如果当前的信息需要保密 30 年，则需要使用 256-bit 或更高的

安全等级。**Zcash 使用的是 128-bit 安全等级。**

那么安全等级是怎么计算的呢？比如说对 AES 加密算法的密文破译，

目前没有明显好于暴力枚举私钥的方式，所以私钥长度为 128 的 AES

算法安全等级是 128-bit, 你只能遍历所有可能的私钥。对于哈希函数

如 SHA256 的碰撞攻击，虽然哈希函数的输出大小为 2

256

, 但是尝试大

概 2 128量级的次数，就有可能找到一组成功的攻击（其原理同“生日攻

击”，23 个人就有一半以上概率在 366 天中有重复的生日），所以，

SHA256 的安全等级是 128-bit. 而对于 RSA 基于的大数分解问题，

由于有远比暴力尝试高效的算法，所以 RSA 中大数的长度需要 3072

bits 才可以达到 128-bit 的安全等级。

**哈希函数**有一些科普文章在介绍哈希函数的时候，只介绍 SHA2, SHA3. 这容易

误导别人觉得只要是哈希函数，都像 SHA2 和 SHA3 那样强大。其实

哈希函数的各种定义有很多，这里介绍其中 3 个。

1. **随机预言机**：这是密码学中的一个理想模型，也算是最强的哈希

函数假设。假设有一个上帝，对相同的输入，它给你相同的输

出，对于若干的不同的输入，它会给出独立随机的结果。著名的

Fiat-Shamir 启发式变换就是用随机预言机把某一类交互式的零

知识证明变成非交互式的。目前 SHA2 和 SHA3 是认为满足最

强的这个假设的，但这只是被普遍接受的假设，而不是有证明的

东西。

2. **反碰撞攻击**：这也是具有密码学安全性的假设，指的是很难构造

出两个不一样的输入，使得他们有相同的输出。区块链系统中常

用的 Merkle Tree 中使用任何反碰撞攻击的哈希函数就够了。

2017 年 2 月，google 构造了两个不同的 pdf 文件，有相同的

SHA1 输出，宣布了 SHA1 生命进入倒计时。但注意，仅仅反

碰撞攻击不代表哈希值可以保护原文数据。如果我定义一个哈希

函数，输出是原文前 10 个字加 SHA2 结果，也是反碰撞攻击

的。

3. **成对独立随机**：这个假设是没有任何密码学性质的，大概指的

是，假设我手里有一些不同的哈希函数，对任何给定的两个输

入，从手里的哈希函数随机抽一个，输出结果应当是独立且随机

的。一组简单的线性函数在同余意义下就可以实现这个性质。