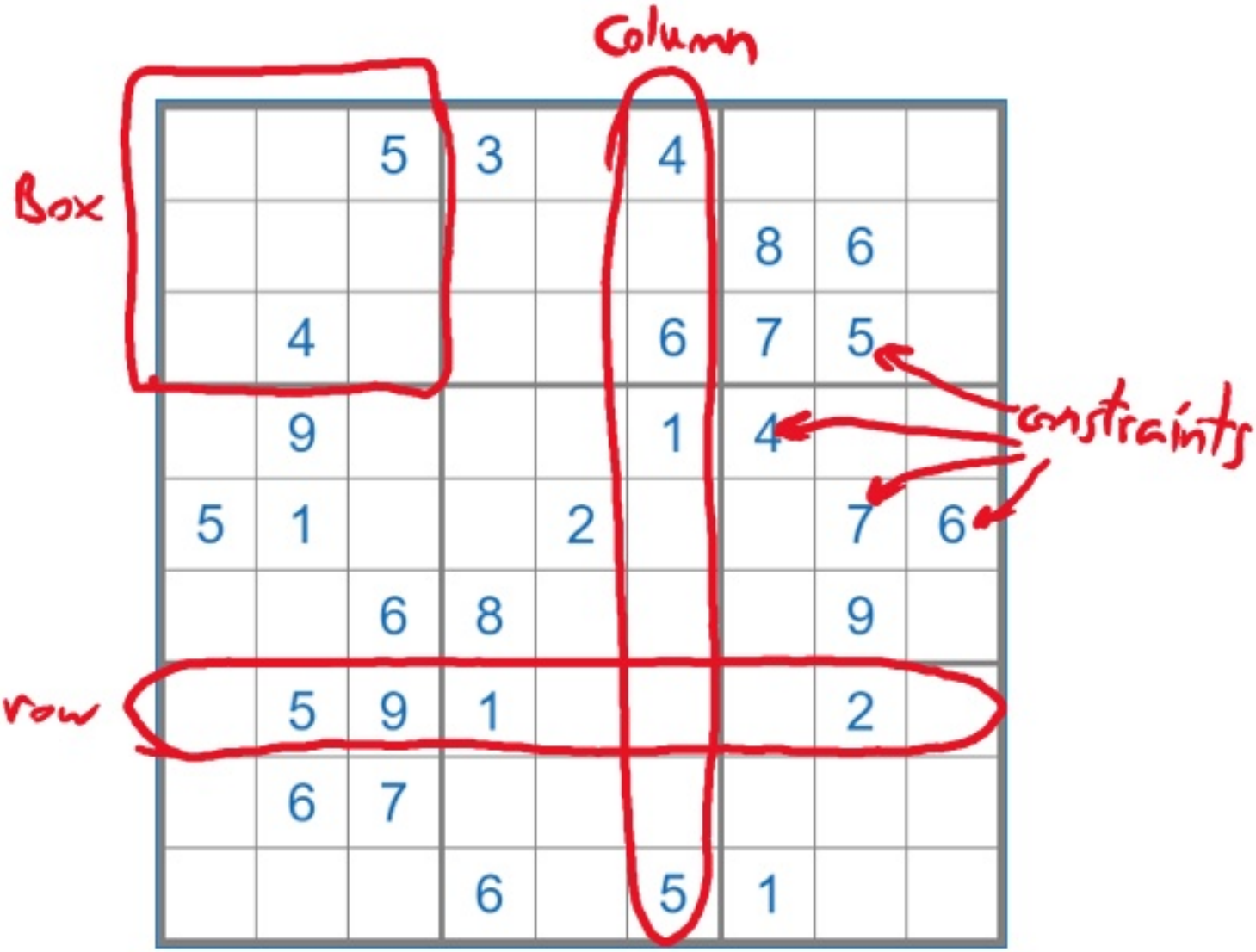


一个数独引发的惨案：零知识证明（Zero-Knowledge Proof）

Xiaoyao ...
安德鲁米勒大弟子

这篇文章大部分译自：medium.com/qed-it/the-i... 原文的作者是著名的Ghost和Spectre 这两个协议的创始团队的领队Aviv Zohar。原文作者说他的这篇原文又是引用了以下这两篇学术论文：

1. *How to Explain Zero Knowledge Protocols to Your Children (Quisquater et. al.)*
2. *Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles (Gradwohl et. al.).*

老钱觉得原文是零知识证明方面写的最好最接地气的科普类的文章。所以想要翻译一下，顺便在原文基础上加上一些自己的解读。想要了解零知识证明，或者匿名性极强的区块链加密货币ZCash的朋友不妨读一读。

小明，小红，小刚三个好朋友很喜欢玩数独。平日里他们三个也会互相出题给对方做。有时候他们会出一些非常变态的数独题互相挑战。他们会挑一个人在纸上画出一个NxN的格子，填上谜面（Constraint），然后交给另外两人去解。

证明

有一天，小明出了一道非常难的数独题，小红花了很长时间尝试去解开这个数独，但是怎么都解不出结果。小红觉得小明在耍她，“这题压根就无解！小明你耍我！”，她跑到小明那抱怨。

“呵呵，我能证明给你看这题是有解的，而且我知道这个解“，小明淡定的回答道。

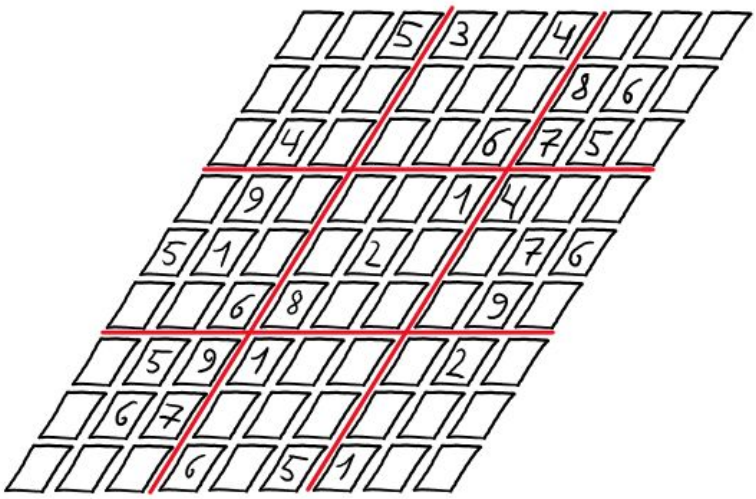
“好啊“，小红暗自想着，“哼哼，等你证明给我看之后，我就把解记下来然后去戏耍一下小刚，给他也做一下这题。”

小明接着说：“我会用零知识证明的方法给你证明我会这题的解。也就是说我不会把解给你看，却能让你信服我确实有这题的解。”

小红并不相信他能这样做到，还在想象小刚被耍的样子。

承诺

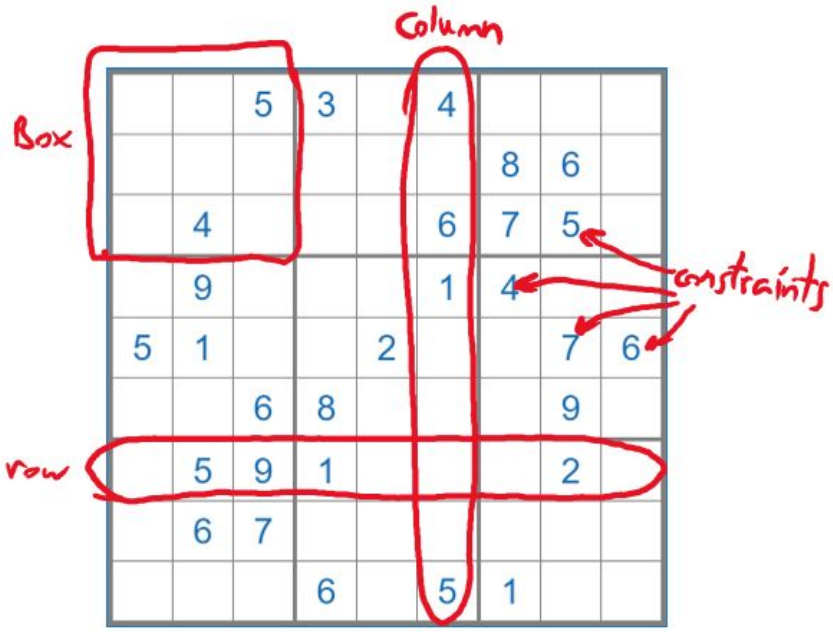
小明拿出81（9x9）张空白的卡片放在桌上，在每张纸上写上1-9中的一个数字，他让小红转过身闭上眼，然后把这81张卡片小心翼翼地按照解的排列放在桌上，代表谜底的卡片，数字面朝下放在桌上；代表谜面的卡片，则数字面朝上放在桌上。



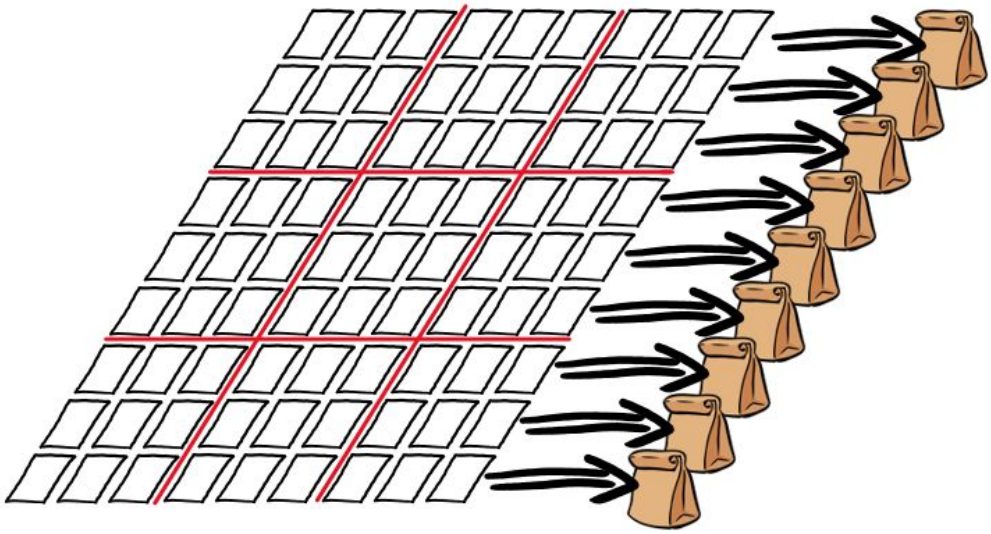
随机试验

小明放好卡片后，让小红睁开眼转过身。小红很激动，她觉得谜底就要揭晓了，很是开心。她可花了好几天时间都没能解出这题。

小明对小红说：“小红，你不能偷看这些面朝下的卡片。“，明显能看出小红很失望，她以为能看到完整的一个解。“但是我能让你检验这些解：你可以随意选择按照行(row)，或者按照列(column)，或者按照3x3的九宫格(box) 来检验我的解。你挑一种吧～”



小红很困惑，嘴上念叨着什么鬼心里想着mmp，然后告诉小明她决定选择按照行的方法来验证，小明接着把每一行的9张卡片收起来单独放到一个麻布袋里。所有卡片都被收完放在了9个麻布袋里。小明接着摇了摇每个麻布袋，把里面的卡片顺序都打散。最后把这9个麻布袋交给小红。



验证

“好了，你可以打开这些布袋了。“小明对小红说，“每个布袋里应该都有正好9张，没有重复数字的，分别是数字1-9的卡片。” 小红打开每个布袋一看，还果真是这样。

“可这啥都证明不了啊！我也可以这样做给你看。我只要保证每一行都是1-9这9张卡片，不去管纵列和九宫格里的数字是不是也都是没有重复的不就行了。“小红气急败坏的说道。

小明解释说：“可是我事先也不知道你会选按照行来收集卡片，还是按照列，还是按照九宫格啊。我又不是你肚子里的蛔虫。。。我是按照题解来放置卡片的 你选啥我都没有怕的”

小红想了想，确实，一个数独只有真正正确的解才能保证每一行每一列每一个九宫格里的数字都是没有重复的1-9。小明如果真的在骗她，小明不会那么理直气壮，小红也至少有1/3的概率可以抓到他在骗人。

重复

小红还是不服气。觉得小明仍然有可能在骗她，所以要求小明再把卡片复原，按照原来的方法，重新选。这样接连试了几次，小红每次都选一个不一样的试验方法。试了好多次都是一样的结果。小红这下不得不承认，小明要么运气非常非常好，每次都能押中小红会选择哪种试验方式，要么就是他确实知道题解，（或者小明会读心术能预先知道小红会选什么试验方式）。小红很失望，这么多次试验下来，她还是不知道真正的题解，她只知道每次小明放置卡片的排列里很大几率每行每列每个九宫格确实都是没有重复的1-9，这就说明很大几率这题是有解的，而且小明很大几率确实知道这题的解。

小明把这种零知识证明的方法也给小刚展示了一遍。从此之后三个好友养成了通过零知识证明去证明给对方看自己知道某题解的习惯。毕竟每个人在解题的时候都花了很大功夫，不想轻易地把题解直接告诉对方。虽然每次零知识证明的过程很花时间，但是他们都乐在其中。

席卷全球的数独风暴

逐渐的，小明和小红发现全世界有很多数独爱好者，他俩决定在斗鱼上开一个直播间，直播解数独。为了展现自己的聪明才智，每周开播前，小明在粉丝团里随机抽取一个粉丝递交的数独，直播时，小明会把题解告诉小红，然后由小红用零知识证明的方法向观看直播的老铁们证明这题有解，并且自己知道题解，老铁们纷纷表示666并送上飞机火箭。就这样小明和小红的直播间人气暴涨，两人成为了斗鱼的签约艺人。

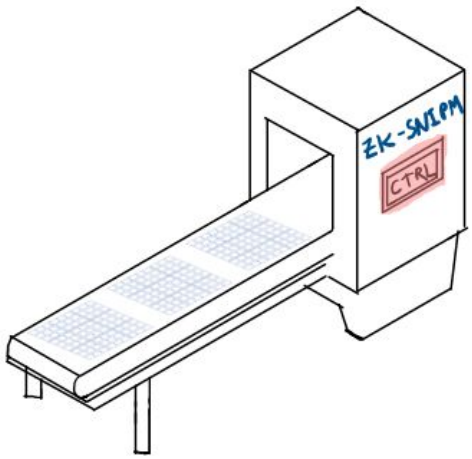
开挂

一天，小明来到小红家准备直播一个非常难的数独，可是他发现他把解出的题解落在自己家了。时间紧迫，要重新算一遍指定赶不上开播时间会被斗鱼老板骂。但是他和小红还是决定开播。开播前小明和小红说：“咱俩假装弄一弄零知识证明，我告诉你一会儿我会怎么选试验方式。你只要确保每次我选的那种试验方式（每行，或每列，或每个九宫格）里的数字不要重复就行了。” 小红同意了。

小刚，在自己家看完了直播，事后小明和小红把他俩这次作假的方法告诉小刚，小刚义愤填膺的斥责他们俩，“你们这样做和卢本伟开挂有什么区别！对得起支持你们的粉丝吗？我再也不相信你们俩的零知识证明了！”

神奇的机器和非交互式证明 (Non-interactive Proofs)

小刚很不爽。一来他很享受之前和小明和小红一起玩数独，但是现在他觉得挂逼不值得信任。小刚想找另一种方法来保证直播中他俩不能再这样作假。几个不眠的夜晚过去之后，小刚告诉小明小红，他想到了一个好方法。小刚把自己关在屋里忙活了一整天，第二天早上他把小明小红叫来，给他们展示自己的新发明：零知识数独非交互式证明机（“The Zero-Knowledge Sudoku Non-Interactive Proof Machine” or zk-SNIPM）。



这台机器基本上就是把小明和小红之前当面做的那套证明自动化，不再需要人为交互。小明只要把卡片放在传送带上，机器会自动选择按行，或列，或九宫格来收取卡片，放到袋子里打乱顺序，然后把袋子通过传送带再送出来。然后小明就可以当着镜头的面拆开袋子展示里面的卡片。

这台机器有一个控制面板，打开里面是一串旋钮，这些旋钮用来指示每次试验的选择（行，列，九宫格）。

小刚已经设置好了试验的序列，然后把控制面板焊死，以保证小明和小红不会知道他到底选择了怎么样一个试验序列。

这下小刚很放心，他可以完全信任自己这台机器，放心的把机器交给小明和小红，让他俩下次直播就直接用这台机器来证明。小刚相信有了这台机器他俩就没法再开挂了。

仪式

小明和小红很嫉妒小刚的这台机器，并且想也能用这台机器来验证小刚自己出的数独题。但是问题是，小刚是知道自己选了什么样的试验序列的，如果用同一台机器去验证小刚自己的数独题解，小刚就可以开挂。小明把大伙聚集起来提议让小刚把控制面板重新打开，然后大家一起来设置控制面板上的试验序列。小明把这个过程称为“可信任的初始设置仪式（trusted setup ceremony）”。

小明提议把这台机器放在一个漆黑的屋子里，把旋钮上的指示贴纸都撕去。他们三人分别进入这个屋子，小红还提议大家进房间时蒙上眼来保证随机性，并且带一顶锡纸做的金属帽子（小红还是怀疑小明多少会一点读心术，想通过锡纸帽子来屏蔽脑电波信号防止读心术（side-channel attack））。这样，最后这些旋钮所代表的试验序列他们三个人都没有办法知道。就算他们3人中有2人事先商量好自己会怎么选，他们也无法得知第三个人会怎么选。仪式结束之后，他们一起把控制面板焊死。

破解这台机器?

一天下午，小红和小刚出去玩儿了。小明一个人在家守着这台机器。他开始琢磨它是不是像小刚说的那样安全可靠。过了一会，他开始给机器故意传送一些假的题解（只保证每行或每列或每九宫格的数字不重复），试图通过这种试错来找出机器里设置的试验序列。慢慢的，小明把机器里的试验序列都推断出来了。他既兴奋又沮丧，你能帮小明设计一个更好的证明机吗?

透过故事看本质

故事讲完了，相信大家对零知识证明有了一个大概的印象。零知识证明的本质就是在**不揭晓**我所知道或拥有的某样东西的前提下，向别人**证明**我有**很大几率（这点很重要，零知识证明说到底是一个概率上的证明）**确实知道或拥有这个东西。

故事里要证明的东西就是一个数独题的解，小明让小红每次随机抽取行，列，九宫格的卡片，并收集在一起随机打乱，小红通过拆开袋子并不能知道题解，但是却能相信小明很大几率确实知道题解。

这个故事里的zk-SNIPM也是半开玩笑地暗指了零知识证明现在最普遍的zk-SNARKs（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge）算法。故事中的zk-SNIPM虽然存在漏洞，但是他还有改进的余地，比如用一台扫描仪把第一次卡片的组合就全扫描下来，然后一次性同时验证所有的试验序列。这样就很难通过试错的方式来破解机器。

小明和小红之间最开始那种互动式的证明方法暗指的是交互式零知识证明（*interactive* zero-knowledge proof）。交互式零知识证明需要验证方（小红）在证明方（小明）放好答案（commitment）后，不断的发送随机试验。如果验证和证明双方事先串通好，那么他们就可以在不知道真实答案的情况下开挂（simulate/forge a proof）。

非交互式的证明则不需要这种互动。但是会额外需要一些机器或者程序，并且需要一串试验序列，这个试验序列不能被任何人知道。有了这么一个程序和试验序列，证明机就能自动算出一个证明，并且能防止任何一方作假。

主打匿名性的区块链加密货币ZCash里用到了零知识证明来保证交易双方和交易金额的匿名性。ZCash团队举行过2次故事中的那种仪式，第一次仪式他们甚至拍摄了一个纪录片，第二次仪式中一组人甚至不惜代价去切尔诺贝利核事故发生地取来了带有核辐射的废料，然后在高空中用利用核辐射来生成随机数。 有兴趣的各位可以去看看ZCash仪式的相关资料，非常有趣。

老钱打算接下去再写几篇关于零知识证明的系列文章，继续介绍零知识证明的正式定义，在以太坊中的应用，以及zk-SNARKs的一些细节。

作者简介：

老钱（BS'14, MS'18），UIUC计算机科学系硕士。师承Zcash Andrew Miller。3年互联网工作经验。目前担任NAD Grid（nadgrid.com）技术合伙人。NAD Grid互联能源世界。

编辑于 2018-03-04

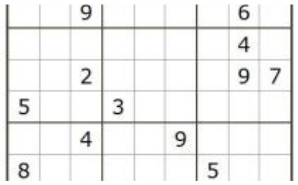
区块链(Blockchain) 零知识证明 ZCash

文章被以下专栏收录

区块链福音战士
我们的信条是“三个拒绝”和“三个拥抱” — 拒绝恐惧、拒绝投机、拒绝盲从； 拥...

进入专栏

推荐阅读



python挑战骨灰级难度数独

Python项目实战

数独求解算法

最近又重新翻出了数独，然后解传说中最难数独没解开（半小时），就萌生了计算机求解的想法。背景交代完毕，然后就开始了苦逼的编码过程。 知乎上找了半天都是DLX，DFS，剪枝...也找到了一些...

刘芒

白话零

Vivi Che

43 条评论 切换为时间排序

写下你的评论...

知乎用户 回复 知乎用户 5 个月前

显然会首先校验初始就有的数字与解的对应位置的数字是否一样

9 查看对话

Jiyu Zhang 回复 周沛源 5 个月前

因为interactive proof就是概率型的而不是确定型的...

1 查看对话

Bert Young 回复 周沛源 5 个月前

然而连续测试10次，差不多就只有六万分之一的概率骗过对方。

赞 查看对话

Homer 回复 Xiaoyao Qian (作者) 5 个月前

期待，好久没在知乎看到这么深入浅出的文章了

2 查看对话

Xiaoyao Qian (作者) 回复 知乎用户 5 个月前

阿里巴巴那个例子不能体现出零知识证明的概率性，其实我觉得不怎么适合

2 查看对话

以上为精选评论

知乎用户

我觉得拿数独的例子来举例并不好……因为我只要随便给个其他题的正确解就能通过校验，因此这并不能说明我解开了那道题。

3

朽木 5 个月前

学习了。。

赞

周沛源 5 个月前

数独的例子还是有1/3的几率骗过对方，不是很严谨

1

观察者 5 个月前

おもしろい

赞

知乎用户 5 个月前

摆三套一样的解（捂脸）

1

胡宇光 回复 知乎用户 5 个月前

这里面好几个动作都难以编程实现。假设A,B是两个节点。你怎么做到“首先校验初始就有的数字与解的对应位置的数字是否一样”？A混淆之后，B怎么能确定混淆后的9张卡片就是他指定的第一行的9张？ 后面描述的那台机器的输入是什么？看上去像是答案。如果这台机器作恶，它根本不混淆，它就能得到答案。

5 查看对话

Xiaoyao Qian (作者) 回复 胡宇光 5 个月前

好问题！我会在后续的几篇文章里详细讲这个具体在实现里是怎么解决的，还有一些安全模型，包括ZCash的ceremony到底是在干什么，什么是ceremony之后的toxic waste。尽情期待！

2 查看对话

简单小煜 回复 知乎用户 5 个月前

文章说了，题面卡片是正着放，题解卡片是反着放

赞 查看对话

何乐不为 5 个月前

可以解决阿里巴巴被四十大盗劫持后，如何保证自己在交出宝藏后不被杀人灭口

1

寇申 5 个月前

写的太好了

赞

好大一只猫丶 5 个月前

疯子了

赞

知乎用户 5 个月前

并不觉得好,还是阿里巴巴和四十大盗的例子比较感人~
最近也在研究zcash的那套东西~

赞

zhang peter 5 个月前

学习了

赞

周沛源 回复 Bert Young 5 个月前

连续测10次？如果3种方式的答案都被知道了，那就可以还原出答案

赞 查看对话

jialin zhong 5 个月前

一般都是阿里巴巴和四十大盗的例子

赞