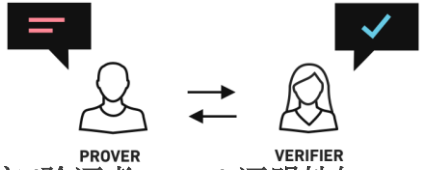
零知识证明

--区块链中的一种方法

讲座大纲

定义

的方法



- **在密码学中, 零知识证明或零知识协议是一种方法, 通过这种方法, 一方 (证明人 peggy) 可以向另一方 (验证者 victor) 证明她知道值 x, 而不传递任何信息, 除了她知道值 x。**
- 另一种理解的方法是: 交互式零知识证明需要个人 (或计算机系统) 之间的互动, 以证明他们的知识和个人验证证明。
- 如果证明语句需要验证者了解一些秘密信息, 则该定义意味着验证者将无法依次向其他人证明该语句, 因为验证者不拥有秘密信息。请注意, 被证明的语句必须包括证明者具有这种知识的断言 (否则, 该语句将不会在零知识中被证明, 因为在协议结束时, 验证者将获得证明者所获得的附加信息了解所需的机密信息)。如果陈述只包含了证明人拥有秘密信息的事实, 那就是一种被称为知识零知识证明的特例, 它很好地说明了零知识证明概念的本质: 证明自己拥有知识如果允许一个人简单地透露某些信息, 则这些信息是微不足道的;挑战在于证明一个人在不透露秘密信息或其他任何信息的情况下就有这样的知识。
- 对于知识的零知识证明, 协议必须需要交互式输入通常以挑战或挑战的形式, 以便验证者的答复在陈述属实的情况下, 并且只有在陈述属实的情况下 (即, 如果证明人确实知道所声称的知识), 才会说服验证者。这显然是事实, 因为否则验证者可以记录协议的执行情况, 并将其重播给他人: 如果这被新的一方接受作为证据, 重播方知道秘密信息, 那么新的一方的接受是无论是合理的-重播确实知道秘密信息--这意味着协议泄露知识, 不是零知识, 或者是虚假的--即导致一方接受某人的知识证明, 而这些证明并不实际拥有它。

定义 (1)

零知识证明必须满足三个属性:

- **完整性**: 如果陈述属实, 诚实的验证者 (即正确遵循协议的人) 将被诚实的验证者相信这一事实。
- **稳健**:: 如果陈述是错误的, 任何欺骗证明者都无法让诚实的验证者相信它是真实的, 除非有一些小的概率。
- **零知识**: 如果语句为真, 则除了语句为真之外, 没有任何验证者会学到任何其他内容。换句话说, 仅仅知道陈述 (而不是秘密) 就足以想象一个场景, 表明证明者知道秘密。这是通过显示每个验证程序都有一些*模拟*只要要证明的陈述 (而且不能接触证明者), 就能产生一份 "看起来像" 诚实的证明者和有关验证者之间的互动的文字记录。

- 前两个是更一般的交互式证明系统的属性。第三是使证明零知识的原因。
- 零知识证明不是证明在数学意义上的术语, 因为有一些小的概率, *健全性错误*, 欺骗的证明者将能够说服验证者的错误陈述。
- 换句话说, 零知识证明是概率 "证明", 而不是确定性证明。但是, 有一些技术可以将稳健性误差降低到可忽略的小值。

定义 (2)

A formal definition of zero-knowledge has to use some computational model, the most common one being that of a Turing machine. Let P,V, and S be Turing machines. An interactive proof system with (P,V) for a language L is zero-knowledge if for any probabilistic polynomial time (PPT) verifier $\hat{V}$ there exists a PPT simulator S such that

$$\forall x \in L, z \in \{0,1\}^*, \mathrm{View}_{\hat{V}}\left[P(x) \leftrightarrow \hat{V}(x,z)\right] = S(x,z)$$

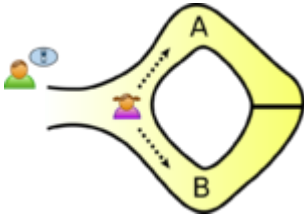
where $\mathrm{View}_{\hat{V}}\left[P(x) \leftrightarrow \hat{V}(x,z)\right]$ is a record of the interactions between $P(x)$ and $\hat{V}(x,z)$. The prover P is modeled as having unlimited computation power (in practice, P usually is a probabilistic Turing machine). Intuitively, the definition states that an interactive proof system (P,V) is zero-knowledge if for any verifier $\hat{V}$ there exists an efficient simulator S (depending on $\hat{V}$) that can reproduce the conversation between P and $\hat{V}$ on any given input. The auxiliary string z in the definition plays the role of "prior knowledge" (including the random coins of $\hat{V}$). The definition implies that $\hat{V}$ cannot use any prior knowledge string z to mine information out of its conversation with P, because if S is also given this prior knowledge then it can reproduce the conversation between $\hat{V}$ and P just as before.

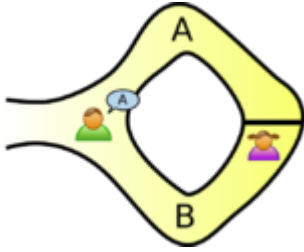
The definition given is that of perfect zero-knowledge. Computational zero-knowledge is obtained by requiring that the views of the verifier $\hat{V}$ and the simulator are only computationally indistinguishable, given the auxiliary string.

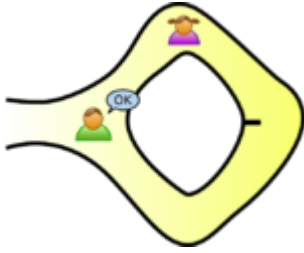
抽象示例

阿里巴巴洞穴

- 有一个著名的故事, 提出了零知识证明的基本思想, 首次出版让-雅克奎斯克特和其他人在他们的论文 "如何解释零知识协议给你的孩子"。通常的做法是将双方标记为 peggy (**普罗弗**声明) 和维克多 (**验证**声明)。
- 在这个故事中, 佩吉发现了这个用来在洞穴中打开魔法门的秘密词。洞里的形状像一个戒指, 一边是入口, 另一侧是神奇的门, 挡住了另一侧。维克多想知道佩吉是否知道这个秘密词;但佩吉是一个非常私人的人, 她不想向维克多透露她的知识 (秘密词), 也不想向全世界透露她的知识事实。
- 他们给从 a 和 b 入口的左右路径贴上标签。首先, 当佩吉走进洞穴时, 维克多在洞穴外等候。佩吉走的要么是 a 路, 要么是 b 路;维克多不允许看她走哪条路。随后, 维克多进入洞穴, 喊着他希望她用来返回的路径的名字, 要么是 a, 要么是 b, 随机选择。如果她真的知道神奇的词, 这很容易: 如果有必要, 她会打开门, 沿着想要的道路返回。
- 然而, 假设她不知道这个词。然后, 只有维克多说出她所走的路的名字, 她才能从指定的小路回来。由于维克多会随机选择 a 或 b, 她有50% 的机会正确猜测。如果他们多次重复这个把戏, 比如连续 2 0次, 她成功预测维克多所有要求的机会就会变得微不足道 (约万分之一)。
- 因此, 如果佩吉反复出现在维克多的出口名字, 他可以得出结论, 它是非常有可能的-在天文学上的可能性-佩吉确实知道这个秘密词。
- 关于第三方观察员的一面说明是: 即使维克多戴着一个隐藏的相机记录着整个交易, 相机唯一会记录的就是维克多在一个案例中喊 "a!", 佩吉出现在 a, 在另一个案例中, 维克多喊 "b!"佩吉出现在 b这种类型的录音对于任何两个人来说都是微不足道的 (只需要佩吉和维克多事先就维克多会喊的 a 和 b 的顺序达成一致)。这样的录音, 除了最初的参与者之外, 肯定永远不会让任何人信服。事实上, 即使是一个以观察者身份在场的人*在最初的实验*会不相信, 因为维克多和佩吉可能已经精心策划了整个 "实验" 从开始到结束。
- 进一步注意, 如果维克多选择他的 a 和 b 的翻转硬币相机, 这个协议失去了它的零知识属性;相机上的硬币翻转可能会让任何后来看录音的人信服。因此, 尽管这并没有揭示维克多的秘密词, 但它确实使维克多有可能使全世界相信佩吉拥有这种知识--这与佩吉宣称的愿望背道而驰。然而, 数字密码学通常是 "翻转硬币" 依靠伪随机数生成器, 这类似于一枚硬币, 其头部和尾部的固定模式只有硬币的主人才知道。如果维克多的硬币有这样的行为, 那么维克多和佩吉也有可能伪造 "实验", 所以使用伪随机数生成器不会以同样的方式向世界揭示佩吉的知识, 使用翻转的硬币会。
- 请注意, 佩吉可以向维克多证明, 她知道这个神奇的词, 而不透露给他, 在一个单一的审判。如果维克多和佩吉一起走到洞口, 维克多就可以看着佩吉通过 a 进去, 从 b 中出来。这将肯定地证明佩吉知道神奇的词, 而没有透露神奇的词维克多。然而, 这种证据可以由第三方观察, 也可以由 victor 记录, 这种证据对任何人来说都是令人信服的。换句话说, 佩吉声称自己与维克多勾结, 无法反驳这样的证据, 因此她已经无法控制谁知道她的知识。







两个球和色盲朋友

- 此示例需要两个具有不同颜色的相同对象, 例如两个彩色球, 它被认为是交互式零知识证明如何工作的最简单的解释之一。它是首次演示现场由软件工程师康斯坦丁诺斯沙尔基亚斯和迈克·赫恩在2017年9月的区块链相关会议上, 受到教授工作的启发。奥布 戈尔德雷希, 谁使用两个不同的彩色卡.
- 想象一下, 你的朋友是色盲, 你有两个球: 一个是红色的, 一个是绿色的, 但在其他方面是一样的。对你的朋友来说, 它们看起来完全一样, 他怀疑它们是否真的可以区分。你想*向他证明, 他们其实是不同的颜色*, 但没有别的, 因此你不透露哪一个是红色的, 哪个是绿色的。
- **这是证明系统。你把这两个球给你的朋友, 他就把它们放在背后。接下来, 他拿了其中一个球, 从背后拿出来, 展示出来。然后这个球又被放在他的背后, 然后他选择只露出两个球中的一个, 切换到*其他*球与概率50%。他会问你: "我换球了吗"然后根据需要经常重复整个过程。**
- 通过看他们的颜色, 你当然可以肯定地说他是否换了它们。另一方面, 如果它们是相同的颜色, 因此无法区分, 你就无法正确猜测概率高于50%。
- 如果你和你的朋友多次重复这个 "证明" (例如 128), 你的朋友应该确信 ("完整性") 球确实是不同的颜色;否则, 您将随机成功识别所有交换机/非交换机的概率接近零 ("健全性")。
- 以上证明是*零知识*因为你的朋友永远不知道哪个球是绿色的, 哪个是红色的;事实上, 他对如何区分球一无所知。

实例

给定值的离散日志 (1)

我们可以将这些想法应用到更现实的加密应用中。佩吉想向维克多证明她知道离散日志给定值的给定值组.

For example, given a value y, a large prime p and a generator g, she wants to prove that she knows a value x such that $g^x \bmod p = y$, without revealing x. Indeed, knowledge of x could be used as a proof of identity, in that Peggy could have such knowledge because she chose a random value x that she didn't reveal to anyone, computed $y = g^x \bmod p$ and distributed the value of y to all potential verifiers, such that at a later time, proving knowledge of x is equivalent to proving identity as Peggy.

The protocol proceeds as follows: in each round, Peggy generates a random number r, computes $C = g^r \bmod p$ and discloses this to Victor. After receiving C, Victor randomly issues one of the following two requests: he either requests that Peggy discloses the value of r, or the value of $(x + r) \bmod (p - 1)$. With either answer, Peggy is only disclosing a random value, so no information is disclosed by a correct execution of one round of the protocol.

Victor can verify either answer; if he requested r, he can then compute $g^r \bmod p$ and verify that it matches C. If he requested $(x + r) \bmod (p - 1)$, he can verify that C is consistent with this, by computing $g^{(x+r) \bmod (p-1)} \bmod p$ and verifying that it matches $C \cdot y \bmod p$. If Peggy indeed knows the value of x, she can respond to either one of Victor's possible challenges.

If Peggy knew or could guess which challenge Victor is going to issue, then she could easily cheat and convince Victor that she knows x when she does not: if she knows that Victor is going to request r, then she proceeds normally: she picks r, computes $C = g^r \bmod p$ and discloses C to Victor; she will be able to respond to Victor's challenge. On the other hand, if she knows that Victor will request $(x + r) \bmod (p - 1)$, then she picks a random value r', computes $C' = g^{r'} \cdot (g^x)^{-1} \bmod p$, and discloses C' to Victor as the value of C that he is expecting. When Victor challenges her to reveal $(x + r) \bmod (p - 1)$, she reveals r', for which Victor will verify consistency, since he will in turn compute $g^{r'} \bmod p$, which matches $C' \cdot y$, since Peggy multiplied by the inverse of y.

However, if in either one of the above scenarios Victor issues a challenge other than the one she was expecting and for which she manufactured the result, then she will be unable to respond to the challenge under the assumption of infeasibility of solving the discrete log for this group. If she picked r and disclosed $C = g^r \bmod p$, then she will be unable to produce a valid $(x + r) \bmod (p - 1)$ that would pass Victor's verification, given that she does not know x. And if she picked a value r' that poses as $(x + r) \bmod (p - 1)$, then she would have to respond with the discrete log of the value that she disclosed – but Peggy does not know this discrete log, since the value C she disclosed was obtained through arithmetic with known values, and not by computing a power with a known exponent.

因此, 欺骗证明者在一轮中成功欺骗的概率为0.5。通过执行足够多的回合, 欺骗程序成功的概率可以被任意降低。

给定值的离散日志 (2)

简短的总结

Peggy proves to know the value of x (for example her password).

1. Peggy calculates first for one time the value $y = g^x \mod p$ and transfer the value to Victor.
2. Peggy repeatedly calculates a random value r and $C = g^r \mod p$. She transfers the value C to Victor.
3. Victor asks Peggy to calculate and transfer the value $(x + r) \mod (p - 1)$ or simply to transfer the value r. in the first case Victor verifies $(C \cdot y) \mod p \equiv g^{(x+r) \mod (p-1)} \mod p$. In the second case he verifies $C \equiv g^r \mod p$.

The value $(x + r) \mod (p - 1)$ can be seen as the encrypted value of $x \mod (p - 1)$. If r is true random, equally distributed between zero and $(p - 1)$, this does not leak any information about x (see one-time pad).

大图的哈密顿周期 (1)

- 在这种情况下, 佩吉知道哈密顿循环对于一个大的图 *G*.维克多知道*G*但不是循环 (例如, 佩吉已经产生了*G*并透露给他。在给定大图的情况下, 找到哈密顿周期被认为在计算上是不可行的, 因为它相应的决策版本是已知的np-完整.佩吉将证明, 她知道这个周期, 而不简单地透露它 (也许维克多有兴趣购买它, 但希望验证第一, 或者也许佩吉是唯一一个谁知道这个信息, 并正在证明她的身份, 维克多)。
- 为了表明佩吉知道这个汉密尔顿周期, 她和维克多打了几轮比赛。
- 在每轮比赛开始时, 佩吉创造了*H*, 一个图形, 它是同构自*G*(即*H*就像*G*除了所有顶点都有不同的名称)。因为它是微不足道的转换哈密顿循环之间的同构图与已知的同构, 如果佩吉知道哈密顿循环*G*她还必须知道一个*H*.
- 佩吉承诺*H*.她可以通过使用加密承诺计划.或者, 她可以编号的顶点*H*, 然后为每个边缘*H*写在一张小纸片上, 上面写着边缘的两个顶点, 然后把这些纸面朝下放在桌子上。这个承诺的目的是, 佩吉不能改变*H*而在同一时间维克多没有关于*H*.
- 维克多然后随机选择两个问题之一, 问佩吉。他可以要求她显示同构之间*H*和*G*(请参见图同构问题), 或者他可以要求她显示哈密顿周期*H*.
- 如果佩吉被要求显示, 这两个图是同构的, 她首先发现所有的*H*(例如, 翻过她放在桌子上的所有论文), 然后提供映射的顶点翻译*G*自*H*.维克多可以证实他们确实是同构的。
- 如果佩吉被要求证明, 她知道哈密顿周期*H*, 她翻译她的哈密顿周期*G*到*H*只发现哈密顿循环的边缘这足以让维克多检查*H*确实包含哈密顿周期。

大图的哈密顿周期 (2)

完整性
如果佩吉确实知道 g 中的哈密顿周期, 她就能很容易地满足维克多对从 g 产生 h 的图同构 (她在第一步就承诺了) 或 h 中的哈密顿周期 (她可以通过将同构应用于细胞来构建的) 的需求勒在G).

零知识
佩吉的回答并没有揭示出最初的哈密顿周期G.每一轮, 维克多只会学会h 's 同构G或哈密顿周期H.他需要两个答案为一个单一的H来发现在其中的循环G, 所以信息仍然是未知的, 只要佩吉可以生成一个独特的H每一轮。如果佩吉不知道哈密顿循环G, 但不知何故事先知道什么维克多会要求看到每一轮, 然后她可以欺骗。例如, 如果佩吉提前知道维克多会要求看到哈密顿周期H然后她就可以为一个不相关的图形生成哈密顿周期。同样, 如果佩吉事先知道维克多会要求看到同构, 那么她就可以简单地生成同构图H(其中她也不知道哈密顿周期)。维克多可以自己 (没有佩吉) 模拟协议, 因为他知道自己会要求看什么。因此, 维克多没有得到任何关于哈密顿周期的信息G从每轮披露的信息。

稳健
如果佩吉不知道这些信息, 她可以猜出维克多会问哪个问题, 并生成一个同构图G或哈密顿周期的一个不相关的图, 但因为她不知道哈密顿周期G她不能两全其美有了这个猜测, 她愚弄维克多的机会是2^{-n}, 其中n是数轮数。对于所有现实的目的, 以这种方式用合理的几轮击败零知识证明是完全困难的。

应用

身份验证系统

零知识证明 (zkp) 的研究的动机是:认证一个一方希望通过一些秘密信息 (如密码) 向另一方证明其身份, 但不希望第二方了解任何有关这个秘密的信息的系统。

这就是所谓的 "零知识"知识的证明".但是, 密码通常太小或太随机, 无法在许多方案中使用, 以实现知识的零知识证明。

a 个零知识密码证明是一种特殊的知识零知识证明, 它解决了密码的有限大小。

道德行为

密码协议中零知识证明的一个用途是在维护隐私的同时执行诚实的行为。

大致来说, 这个想法是为了强迫用户使用零知识证明, 证明其行为根据协议是正确的。

由于健全性, 我们知道用户必须真正诚实行事, 才能提供有效的证据。

由于知识为零, 我们知道用户在提供证据的过程中不会泄露其隐私的秘密。

核裁军

2016年, 普林斯顿大学等离子体物理实验室和普林斯顿大学展示了一种可能适用于未来核裁军谈判的新技术。

它将使视察员能够在不记录、分享或披露可能是秘密的内部工作的情况下, 确认一个物体是否确实是核武器。

区块链

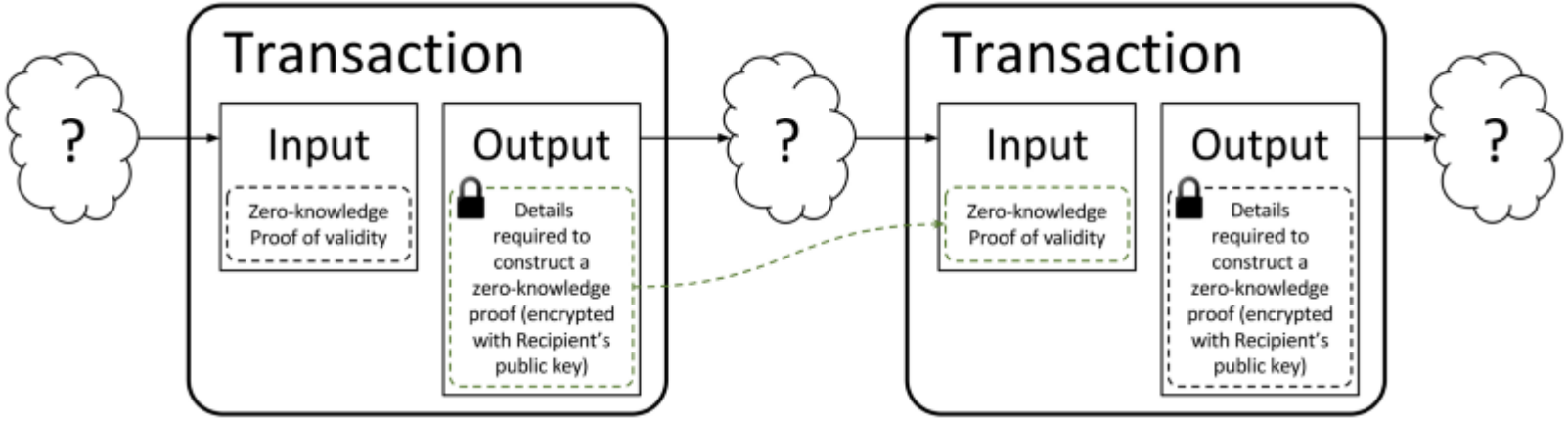
zkp 可用于保证交易有效, 尽管有关发件人、收件人和其他交易详细信息的信息仍然是隐藏的。

零知识协议支持跨分布式对等区块链网络的资产转移, 具有完全的隐私性。在常规区块链交易中, 当资产从一方发送到另一方时, 网络中的每一个其他当事方都可以看到该交易的详细信息。相比之下, 在零知识交易中, 其他人只知道发生了有效的交易, 但不知道发送方、收款人、资产类别和数量。所花费的身份和金额可能仍然是隐藏的, 以及诸如 "前跑"是可以避免的。

使用零知识证明的最突出的基于区块链的系统是扎卡什, 这也是要实现的第一个加密货币Zk-snarks. 其他基于区块链的系统也已纳入零知识证明到他们的解决方案, 允许交易被验证, 同时保护用户/事务隐私。可能是最有名的是以太, 这实现Zk-snark 作为一部分的拜占庭升级.

什么是zk-snarks?

你可能已经偶然发现了这个词 "zk-snarks'.这个词是2012年推出通过Nir 比坦斯基, rancanetti, alessandro chiesa &埃兰 特罗默并描述了零知识技术的一个特殊变体。Zk-snark 推出了许多创新, 使它们可以在区块链中使用。最重要的是Zk-snark 减少了校即用的大小和验证它们所需的计算量。



https://z.cash/zh/technology/zksnarks/

历史

历史 (1)

零知识证明最早是在1985年由沙菲 戈德瓦瑟,贝卢斯科尼米卡利和查尔斯拉克科夫在他们的论文 "交互式证明系统的知识复杂性"。本文介绍了**Ip**交互式证明系统的层次结构 (*看到交互式证明系统*), 并构思了*知识复杂性*, 测量从证明器传输到验证器的证明的知识量。

They also gave the first zero-knowledge proof for a concrete problem, that of deciding quadratic nonresidues mod *m* (this more or less means that there isn't any number *x* where x^2 is "equivalent" to some given number). Together with a paper by László Babai and Shlomo Moran, this landmark paper invented interactive proof systems, for which all five authors won the first Gödel Prize in 1993.

用他们自己的话说戈德瓦瑟,米卡利和拉克科夫说：

> 特别令人感兴趣的是, 这种额外的知识本质上是 0, 我们表明, [它] 是可能的, 以交互方式证明一个数字是二次非残留模式*米*释放0额外的知识。这是令人惊讶的, 因为没有有效的算法来确定二次残差国防部*米*是已知的当*米*不给出分解。此外, 所有已知的*Np*这个问题的证据显示了主要的分解*米*.这表明, 在证明过程中添加交互, 可能会减少为了证明一个定理而必须传达的知识量。

二次非残留问题既有一个**Np**和一个**联合 np**算法, 所以在于在交叉点**Np**和**联合 np**.随后发现零知识证明的其他几个问题也是如此, 例如一个未公布的证明系统。奥布 戈尔德雷希验证双素数模量不是百隆整数.
奥布 戈尔德雷希,贝卢斯科尼米卡利和Avi 维德森更进一步, 表明, 假设存在不可破坏的加密, 可以为 np 完成创建零知识证明系统图形着色问题有三种颜色。因为每一个问题**Np**可以有效地减少到这个问题, 这意味着, 在这个假设下, 所有的问题**Np**有零知识证明。假设的原因是, 与上面的示例一样, 它们的协议需要加密。一个通常被引用的存在不可破坏的加密的充分条件是存在单向函数, 但它是可以想象的, 一些物理手段也可能实现它。

历史 (2)

除此之外, 他们还表明,图非同构问题, 则补充的图同构问题, 有零知识证明。此问题在**联合 np**, 但目前尚不知道在这两个**Np**或任何实际的类。更广泛地说,罗 素伊帕利亚佐和容莫蒂以及 ben-or 等人将继续表明, 也假设单向功能或不可破坏的加密, 有零知识证明*所有*中的问题。**Ip=电子空间**换句话说, 任何可以通过互动证明系统证明的东西都可以用零知识来证明。

不喜欢做不必要的假设, 许多理论家寻求一种方法, 以消除的必要性单向功能.这样做的一个方法是*多协议交互式证明系统*(请参见交互式证明系统), 其中有多个独立的程序, 而不是只有一个, 允许验证者隔离 "盘问" 程序, 以避免被误导。可以证明, 在没有任何棘手的假设的情况下, 所有语言在**Np**在这样的系统中具有零知识证明。

事实证明, 在类似 internet 的环境中, 多个协议可以同时执行, 构建零知识证明更具挑战性。研究并行零知识证明的研究路线是由多哈工作,纳尔和萨海.沿着这些路线的一个特别发展是证人无法区分的证明协议。证人不可理解性的性质与零知识的性质有关, 但证人区分协议并不存在同样的并发执行问题。

零知识证明的另一个变种是非交互式零知识证明.布鲁姆, 费尔德曼, 和米卡利结果表明, 在证明者和验证者之间共享一个共同的随机字符串, 就足以在不需要交互的情况下实现计算的零知识。

2017年9月, 在以太的拜占庭叉子上进行了第一批 zkp 活动。

引用

外部链接

"什么是零知识证明, 为什么它有用？".2017年11月16日。

"以太升级拜占庭是活的, 验证第一个 zk-斯纳克证明".科因电报.检索2017-12-18。

教程由奥布 戈尔德雷希在零知识证明

演示零知识证明在不使用的情况下是如何工作的数学

中。比特币的零知识证明绑定

धन्यवाद

Hindi 印地语

Спасибо

俄语

شكراً

阿拉伯语

格拉齐

意大利语

நன்றி

Tamil

泰米尔语

以任何努力

多谢

繁体中文

谢谢

英语

多谢

简体中文

ありがとうございました

日语

ขอบคุณ

泰语

谢谢

西班牙语

奥布里加多

西葡萄牙语

丹克

德语

谢谢

法语

감사합니다

朝鲜语