# 区块链中的数学--PLookup

区块链中的数学
(https://learnblockchain.cn/tags/%E5%8C%BA%E5%9D%97%E9%93%BE%E4%B8%AD%E7%9A%84%E6%95%B0%E5%AD%A6)
零知识证明 (https://learnblockchain.cn/tags/%E9%9B%B6%E7%9F%A5%E8%AF%86%E8%AF%81%E6%98%8E)
PLONK (https://learnblockchain.cn/tags/PLONK)
密码学 (https://learnblockchain.cn/tags/%E5%AF%86%E7%A0%81%E5%AD%A6)

本文主要介绍plookup算法的思路

# 写在前面

上一篇介绍了MultiSet check& Schwartz–Zippel lemma的应用 (https://learnblockchain.cn/article/2659)，有了基础，可以进一步介绍plookup算法了。

首先看下Plookup的初心。

# Plookup应用

使用zk snark去证明一些程式时，有一类操作不是很友好，比如AES-128 或者 SHA-256，它们包含了大量的位操作（异或，与等），这些位操作要表示成门约束，需要先把数分解成二进制位，然后检验二进制位正确性，然后在执行目标操作，所以传统方法约束较为复杂，直观体现门数量多。

以异或（XOR）操作为例：
假如有三个向量域元素，$a = (a_1, ..., a_n), b = (b_1, ..., b_n), c = (c_1, ..., c_n)$，检验每个元素都是8比特位，而且 $i \in [n], c_i = a_i \bigoplus b_i$

使用lookup table来实现约束的思路比较直接，预计算出8比特位操作数所有的输入输出，构造查找表三项$t_1, t_2, t_3$，前两项是输入，后一项是XOR结果，检验t3是否是正确的操作结果，变成检验$t_1, t_2, t_3$是否是预计算table中的一项(entry)。

检验元组$(a_i, b_i, c_i)$是表中的一项，首先把元组转化为单个元素 $f_i = a_i + rb_i + r^2c_i$, 相应地对table做类似处理, $t_i = t_{i1} + rt_{i2} + r^2t_{i3}$, 如果f属于t, 根据上篇说的Schwarz-Zippel Lemma 可以证实元组在table中。

现在问题转化为证明一个向量（集合）f包含在另一个向量（集合）t中，是plookup协议的核心。

# plookup协议

如果向量f中每个元素都在t中，记为f ⊂ t，假设s是f||t，并且按照t中元素出现顺序排序，可以得出s中包含相同的相邻元素差值，反之亦然。

例如f = {2,2,1,1,5}, t = {1,2,5},那么s = {1,1,1,2,2,2,5,5},
令$t' = t_{i+1} - t_i = \{1, 3\}$, s相邻元素差值 $s' = s_{i+1} - s_i = \{0, 0, 1, 0, 0, 3, 0\}$, 对于f ⊂ t， s'与t'包含相同的非零元素（本例子中{1,3}）。仔细观察s'，可以发现其中0元素的个数是等于f向量元素个数|f|,这是必然的。

## randomness引入

验证f ⊂ t 进一步转化为s', t'包含相同的非零元素，本质上在于验证s,t相邻元素非零差值相同。通过构造随机化差值向量可以实现检验。具体地，令$s' = s_i + \beta s_{i+1}, t' = t_i + \beta t_{i+1}$,
现在可以对s', {(1 + β)f, t'}做多集合相等校验。根据上一节randomness的思想， 将β作为自变量，s' 就是度为1的多项式。
当$s_i \neq s_{i+1}$ 不能对应(1 + β)f任一元素，会对应t'中某一元素$(t_j + \beta t_{j+1})$，因为二者系数结构相同（1，β），意味着s中新的不同元素包含在t中, s ⊂ t。
当$s_i = s_{i+1}$， $s' = (1 + \beta)s_i$， 一定对应于某个$f_j$, 可得f ⊂ s, 间接推出 f ⊂ t .

为什么一开始思路是相邻元素做减法，后面验证却用加法呢？二者本质相同，减法好理解直接对差值做随机化，加法略微有点回路:
假设相减差值集合 $delta = d_1, d_2, ..., d_n, s' = s_i + \beta s_{i+1} = s_i + \beta(s_i + d_i) = (1 + \beta)s_i + \beta d_i$, 可以看出也是对差值做的随机化。
所以说直接用减法结果做多集合校验也是没问题的！具体详细P，V多项式的构造与验证，可以查阅plookup的paper。

# 小结

本文主要介绍plookup算法的思路，本质上是用空间换时间的技巧，预计算一系列范围的值，构造table，验证时验证原始提供的元组（witness）是否在table内，之所以可以这么做的原因到此一目了然！感谢张博从第一性原理角度进行细节分析！

原文链接：https://mp.weixin.qq.com/s/_7LAvH-Rzat337YKL0aWpw (https://mp.weixin.qq.com/s/_7LAvH-Rzat337YKL0aWpw)
欢迎关注公众号：blocksight

## 相关阅读

区块链中的数学 -- MultiSet check& Schwartz–Zippel lemma (https://learnblockchain.cn/article/2659) MultiSet check& Schwartz–Zippel lemma

相关plonk系列视频 (https://mp.weixin.qq.com/mp/appmsgalbum?action=getalbum&__biz=MzA5NzI4MzkyNA==&scene=1&album_id=1664071313331650562&count=3#wechat_redirect)

区块链中的数学 -盲签名（Blind Signature） (https://learnblockchain.cn/article/2527) 盲签名原理

区块链中的数学 - sigma协议OR Proof&签名 (https://learnblockchain.cn/article/2507) sigma协议的扩展--OR proof

区块链中的数学 - 何谓零知识证明? (https://learnblockchain.cn/article/2445) 何谓零知识证明

区块链中的数学 - RSA累加器的非成员证明 (https://learnblockchain.cn/article/2444) RSA Accumulator非成员证明以及区块链应用

区块链中的数学 - Accumulator(累加器) (https://learnblockchain.cn/article/2373) 累加器与RSA Accumulator

区块链中的数学 - Kate承诺batch opening (https://learnblockchain.cn/article/2252) Kate承诺批量证明

区块链中的数学 - 多项式承诺 (https://learnblockchain.cn/article/2165) 多项式知识和承诺

区块链中的数学 - Pedersen密钥共享 (https://learnblockchain.cn/article/2164) Pedersen 密钥分享

区块链中的数学 - Pedersen承诺 (https://learnblockchain.cn/article/2096) 密码学承诺--Pedersen承诺

区块链中的数学 - 不经意传输 (https://learnblockchain.cn/article/2022) 不经意传输协议

区块链中的数学 - RSA算法加解密过程及原理 (https://learnblockchain.cn/article/1548) RSA加解密算法

区块链中的数学 - BLS门限签名 (https://learnblockchain.cn/article/1962) BLS m of n门限签名

区块链中的数学 - BLS密钥聚合 (https://learnblockchain.cn/article/1912) BLS密钥聚合

Schorr 签名基础篇 (https://learnblockchain.cn/article/2450) Schorr签名与椭圆曲线

区块链中的数学-Uniwap自动化做市商核心算法解析 (https://learnblockchain.cn/article/1494) Uniwap核心算法解析（中）



发表于 2021-07-12 11:01 阅读（860） 学分（3） 分类：入门/理论 (https://learnblockchain.cn/categories/basic)



## 你可能感兴趣的文章

关于以太坊账户的理解 (https://learnblockchain.cn/article/3592) 192 浏览

真正理解 Layer2 (https://learnblockchain.cn/article/3580) 757 浏览

聊一聊 zkMove （二） (https://learnblockchain.cn/article/3492) 239 浏览

聊一聊 zkMove（一） (https://learnblockchain.cn/article/3471) 236 浏览

零知识证明 – Halo2电路构建源代码导读 (https://learnblockchain.cn/article/3442) 238 浏览

Plonky2入门指南 ——关于全世界最快的ZK技术 (https://learnblockchain.cn/article/3433) 499 浏览

## 相关问题

bulletproofs的原理 (https://learnblockchain.cn/question/2758) 1 回答

基于区块链的数据交易 (https://learnblockchain.cn/question/2546) 1 回答

【招聘】filecoin算法工程师 (https://learnblockchain.cn/question/2519) 0 回答

关于ECDSA签名的malleability问题 (https://learnblockchain.cn/question/2193) 2 回答

【杭州-招聘】区块链头部公司，坐标未来科技城CBD (https://learnblockchain.cn/question/1809) 0 回答

win10上跑——实践指南：构建一个零知识证明 DApp [译]demo时发生错误 (https://learnblockchain.cn/question/1493) 1 回答

## 0 条评论

请先 登录 (https://learnblockchain.cn/login) 后评论



(https://learnblockchain.cn/people/1514)

**blocksight (https://learnblockchain.cn/people/1514)**
78 篇文章, 2219 学分