区块链中的数学 – Kate承诺

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)

> 与上一篇初步方案相比，Kate承诺实现了多项式的隐藏和部分打开验证，实际上方法1生成的结果在zk-snark项目中称为SRS（structure reference string）或者CRS（common reference string），是承诺方P和验证方V所共有，实际选择曲线配对不是对称的，而是非对称两个群，以后说到具体的项目代码可以看得比较清楚。

写在前面

上一篇介绍了多项式知识和承诺 (https://learnblockchain.cn/article/2165)， 本文继续讲述完整的Kate承诺。

Kate承诺

Kate承诺是Kate，Zaverucha，Goldberg等人在2010年提出的多项式承诺方案。
该方案包含以下六个方法:

1. Setup

选择适当的椭圆曲线，选择对称双线性映射的子群,生成元G, 配对函数$e:G*G=G_T$, 随机选择秘密 α（作用类似于私钥）。
假设目标多项式最大的度是t, 产生t+1 个元组$g, g^{\alpha}, g^{\alpha^2}, ..., g^{\alpha^t}$， 该元组公开（作用类似于公钥）， 并销毁（或者遗忘）α值。

2. Commit

令要承诺的多项式是$\varphi(x)=\sum_{j=0}^{d} a_j x^j$,其中d是ϕ(x)的度且小于等于t,计算承诺$C=\prod_{j=0}^{d}(g^{\alpha^j})$,注意区分$\alpha$与系数a的表示区别.

3. Open(Reveal)

输出初始原始多项式ϕ(x)

4.VerifyPoly

根据已知承诺C，和多项式ϕ(x)，验证承诺，直接代入方法2中即可验证。

5.CreateWitness

给定特定多项式输入i,计算i处多项式的值，令$\psi_i(x) = \frac{\varphi(x)\ \varphi(i)}{x\ i}$, 计算$w_i = g^{\psi_i(\alpha)}$, $(\psi_i(x), w_i)$是i处多项式的值的见证

6.VerifyEval

输入：i处多项式的值$\varphi(i)$， 多项式承诺C，见证w_i
验证：
$e(C, g) = e(w_i, g^\alpha / g^i) * e(g, g)^{\varphi(i)}$
等式成立，则多项式承诺为真。

知其然知其所以然，看看为什么成立?
推导过程：
$e(w_i, g^\alpha / g^i) * e(g, g)^{\varphi(i)}$
$= e(g^{\psi_i(\alpha)}, g^{\alpha - i}) * e(g, g)^{\varphi(i)}$
$= e(g, g)^{\psi_i(\alpha)(\alpha\ i) + \varphi(i)}$
$= e(g, g)^{\varphi(\alpha)}$
$= e(C, g)$

其中用到了方法5，变形得到：$\psi_i(x)(x - i) + \varphi(i) = \varphi(x)$

分析比较

方法1是创建了一个密文空间，使得多项式的输入被隐藏，承诺者P在不知道输入的情况下是难以伪造的，这一点在前一篇文章 (https://learnblockchain.cn/article/2165)末尾分析过。

方法2在密文空间中计算多项式承诺。

方法3属于完全打开（披露）多项式，供验证者验证，这种方式不具有零知识的性质。

方法4用来检验承诺对应的多项式。

方法5用在部分打开（披露）的场景，在需要零知识性质的场景下，验证者不能知晓完整的多项式信息，取而代之，是随机选择输入挑战i，由承诺者P生成i处的多项式值和见证。

方法5检验在输入i处的部分打开（披露），如果通过，则认可承诺C所表示的多项式在i处求值φ(i)是正确的，

与上一篇 (https://learnblockchain.cn/article/2165)初步方案相比，Kate承诺实现了多项式的隐藏和部分打开验证，实际上方法1生成的结果在zk-snark项目中称为SRS（structure reference string）或者CRS（common reference string），是承诺方P和验证方V所共有，实际选择曲线配对不是对称的，而是非对称两个群，以后说到具体的项目代码可以看得比较清楚。
通常setup过程采用MPC安全多方计算来保证安全。

小结

Kate承诺方案还有一种变种形式，详细可以参考其paper，本文讲述的是最常用的形式。

多项式承诺的方案不止Kate方案一种，常用的还有基于FRI的承诺方案，以后如果用到再说吧。

本文参考：
Polynomial Commitments：http://cacr.uwaterloo.ca/techreports/2010/cacr2010-10.pdf

零知识算法解析3--多项式承诺 (https://mp.weixin.qq.com/s?__biz=MzA5NzI4MzkyNA==&mid=2247484435&idx=1&sn=9764bb926f7c373c2f6eeefc11278ba9&channel_session_id=&sessionid=svr_60845abd2a9&scene=21&subscene=136#wechat_redirect)

好了，有了这些铺垫，下一篇 (https://learnblockchain.cn/article/2252)可以继续零知识证明的整体介绍了！

原文链接：https://mp.weixin.qq.com/s/W1Q4VijtEpDIgHX2NiCYrA (https://mp.weixin.qq.com/s/W1Q4VijtEpDIgHX2NiCYrA)
欢迎关注公众号：blocksight

相关阅读

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 - 哈希承诺 (https://learnblockchain.cn/article/2085) 密码学承诺--hash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- BLS 基石（双线性函数）和配对 (https://learnblockchain.cn/article/1963) 双线性映射（配对）

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

区块链中的数学 - BLS数字签名 (https://learnblockchain.cn/article/1905) BLS签名及验证

区块链中的数学 - 参与者 < 门限值t的密钥更新Amir Herzberg方案 (https://learnblockchain.cn/article/1843) Amir Herzberg改进方案

区块链中的数学 - Feldman的可验证的密钥分享 (https://learnblockchain.cn/article/1789) Feldman可验证密钥分享方案

区块链中的数学 - Ed25519签名 (https://learnblockchain.cn/article/1663) Ed25519签名

Schorr签名与椭圆曲线 (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 2021–02–28 17:58 阅读（1584） 学分（3） 分类：入门/理论 (https://learnblockchain.cn/categories/basic)

0 赞 收藏

你可能感兴趣的文章

区块链中的数学--PLookup (https://learnblockchain.cn/article/2732) 859 浏览

区块链中的数学 -- MultiSet check& Schwartz–Zippel lemma (https://learnblockchain.cn/article/2659) 779 浏览

区块链中的数学 – 环签名（ring signature）(https://learnblockchain.cn/article/2567) 1848 浏览

区块链中的数学 –盲签名（Blind Signature）(https://learnblockchain.cn/article/2527) 2076 浏览

区块链中的数学 – sigma协议OR Proof&签名 (https://learnblockchain.cn/article/2507) 961 浏览

区块链中的数学 – sigma协议与Fiat–Shamir变换 (https://learnblockchain.cn/article/2493) 1588 浏览

相关问题

0 条评论

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

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

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