区块链中的数学 – Pedersen密钥共享

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)

> Pedersen基于门限的秘密分享方案实际上采用了Pedersen承诺来构建多项式系数承诺，这一点很容易从对比其他秘密分享方案得出！

写在前面

上一篇介绍了密码学承诺中的Pedersen承诺 (https://learnblockchain.cn/article/2096)，与Pedersen相关的还有一个密钥共享方案，如果你一直关注的话，会知道关于密钥分享之前专门介绍过，从《区块链中的数学》54--- > 61篇，本文要介绍的也属于这一类别。

本文基础就是上述的密钥分享的历史文章，之前内容理解的话，本文顺理成章！

Pedersen 密钥分享

符号约定

G_q是素数P的q阶子群，g,h是其生成元，参与者数量n,
k是门限值, p_i代表第i个参与者， 秘密s, 函数$E(a,b) = g^a h^b$

分发阶段

1. 分发者随机秘密选择r,公布对s的承诺$E\ （s,r）\ = g^s h^r$， 继续选择k个随机数$a_i, i \in [1, k-1]$, 构造多项式: $f(x) = s + \sum_{i=1}^{k-1} a_i x^i$
2. 计算$s_i = f(i)$,产生另一组随机数$b_i, i \in [1, k-1]$, 计算系数a_i的承诺：$E_{a_i} = g^{a_i} h^{b_i}$,并公开该承诺值
3. 构造多项式：$g(x) = r + \sum_{i=1}^{k-1} x^i$

计算$r_i = g(i)$, 将信息（s_i, r_i）发送给参与者P_i

验证阶段

4. 当P_i收到他的秘密份额（s_i, r_i）时,执行验证:
   $E\ （s_i, r_i）\ = \prod_{j=0}^{k-1} E_j^{ij}$
   其中$E_j^{ij} = g^{a_j i^i} h^{b_j i^i}$

密钥恢复阶段

1. 至少 k个参与者正确共享密钥份额时，利用拉格朗日多项式插值法可恢复秘密，这一篇 (https://learnblockchain.cn/article/1788)已经说过具体算法，这里不在赘述！

可以看出函数E起到的是密码学承诺的作用！

关于此方案正确性推导，只要你对之前密钥分享的几篇看明白的话，很容易自己推出！

小结

Pedersen基于门限的秘密分享方案实际上采用了Pedersen承诺来构建多项式系数承诺，这一点很容易从对比其他秘密分享方案得出！

虽然本文用的指数形式表示函数E，也可以如同上一篇Pedersen承诺那样使用椭圆曲线来描述，$E(a,b) = a * g_1 + b * g_2$($g_1, g_2$分别是椭圆曲线上选定的两点)，所以说本文描述的密钥分享方案，是Pedersen承诺的一种应用！

好了，下一篇 (https://learnblockchain.cn/article/2165)继续密码学承诺的其他内容！

原文链接：https://mp.weixin.qq.com/s/X09Fdgrzpuo9ia7B4nIdNQ
(https://mp.weixin.qq.com/s/X09Fdgrzpuo9ia7B4nIdNQ)
欢迎关注公众号：blocksight

相关阅读

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

区块链中的数学-ElGamal算法 (https://learnblockchain.cn/article/1557) ElGamal算法签名及验证&实例演练

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）

本文参与登链社区写作激励计划 (https://learnblockchain.cn/site/coins)，好文好收益，欢迎正在阅读的你也加入。

发表于 2021-02-13 12:47 阅读 (1590) 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)

©2022 登链社区 (https://learnblockchain.cn) 版权所有 | Powered By Tipask3.5 (http://www.tipask.com) | 站长统计 (https://www.cnzz.com/stat/website.php?web_id=1265946080)
粤公网安备 44049102496617号 (http://www.beian.gov.cn) 粤ICP备17140514号 (http://beian.miit.gov.cn)