区块链中的数学 – Pedersen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)

Pedersen承诺产生方式，有些类似加密，签名之类的算法。但是，作为密码学承诺重在“承诺”，并不提供解密算法，即如果只有r，无法有效地计算出隐私数据v。

写在前面

上一篇介绍了密码学承诺中的hash承 (https://learnblockchain.cn/article/2085)，也是最简单的承诺方式，本文继续讲用途更广泛的Pedersen承诺！

Pedersen Commitment

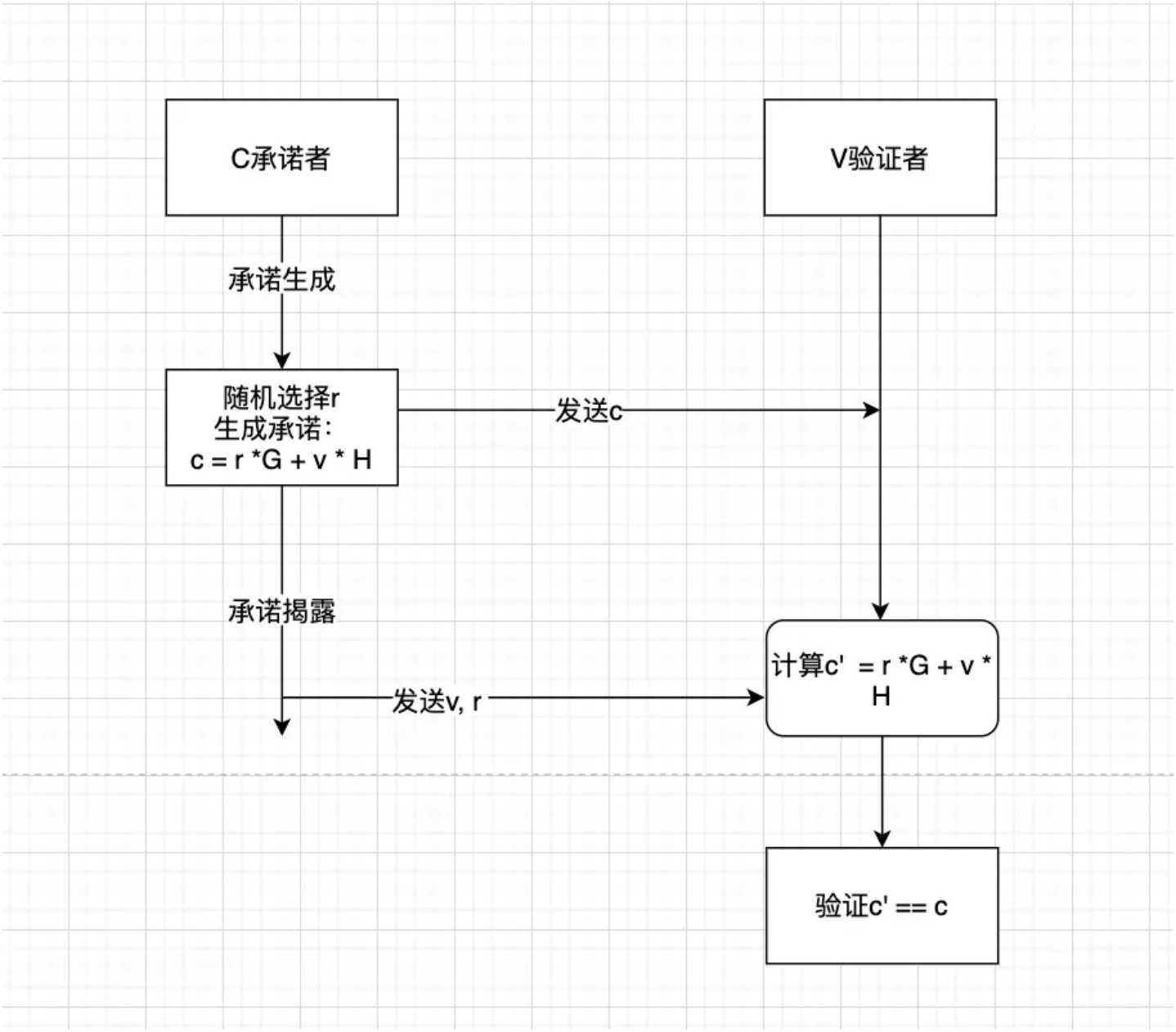
Pederson承诺是密码学中承诺的一种，1992年被Torben Pryds Pedersen在“Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing”一文中提出。
目前Pedersen Commitment主要搭配椭圆曲线密码学使用（当然也可以结合指数运算）。具有**基于离散对数困难问题的强绑定性和同态加法特性的密文形式**。

以结合椭圆曲线为例来说明，Pedersen承诺核心公式表达：

C = r * G + v * H

上述公式中，C为生成的承诺值，G、H为特定椭圆曲线上的生成点，r代表着盲因子（Blinding factor），v则代表着原始信息。由于G、H为特定椭圆曲线上的生成点，所以r * G、v * H可以看作是相应曲线上的公钥（r、v同理也可以视为私钥）。

承诺生成和揭露过程如图：



由于引入了随机盲因子r，对于同一个v会就能产生不同的承诺c，即便敏感隐私数据v不变，最终的承诺c也会随着r的变化而变化，因此提供了信息论安全的隐匿性。这一点类似ECDSA，Schnorr签名采用的手法。

Pedersen承诺加法同态

Pedersen承诺还具有加法同态特性。所谓加法同态，即两数相加和的密文等于两数的密文相加！假设明文a, b ,加密函数e，满足:
c = a + b
e(a) + e (b) = e(c)

Pedersen承诺结合椭圆曲线天然地具备了加法同态的特性，这是椭圆曲线点运算的性质决定的。

假设有两个要承诺的信息v_1, v_2, 随机数r_1, r_2,生成对应的两个承诺:
$C(v_1) = r_1 * G + v_1 * H$
$C(v_2) = r_2 * G + v_2 * H$

则$v_1 + v_2$承诺结果：

$$C(v_1 + v_2) = (r_1 + r_2)G + (v_1 + v_2) * H$$
$$(r_1 G + v_1 * H) + (r_2 * G + v_2 * H)$$
$$C(v_1) + C(v_2)$$

Pedersen承诺还可以扩展构造$v_1 * v_2$等复杂的情况，来证明新产生的承诺满足与原始承诺之间存在指定的约束关系。

小结

Pedersen承诺产生方式，有些类似加密，签名之类的算法。但是，作为密码学承诺重在“承诺”，并不提供解密算法，即如果只有r，无法有效地计算出隐私数据v。

目前Pedersen承诺在区块链中的应用主要在隐私币中，如zcash,MimbleWimble,Monero等。

其他业务系统中，适用于数据源向第三方证明承诺中的秘密数据满足一定的约束关系，其实这也是所有密码学承诺的主要的应用场景！

既然说到了Pederson承诺，Pederson还有一个可验证的密钥分享方案，下一节(https://learnblockchain.cn/article/2164)继续说说吧！

原文链接：https://mp.weixin.qq.com/s/BVXgJE-rL8_r8n1xB5J-JA (https://mp.weixin.qq.com/s/BVXgJE-rL8_r8n1xB5J-JA)

欢迎关注公众号：blocksight

相关阅读

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

区块链中的数学-VRF基于ECC公钥体制的证明验证过程 (https://learnblockchain.cn/article/1582) 基于椭圆曲线的VRF证明验证过程

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 2021–02–02 13:33 阅读（ 3116 ） 学分（ 9 ） 分类：入门/理论 (https://learnblockchain.cn/categories/basic)

1 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)