区块链中的数学 – BLS 基石（双线性函数）和配对

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)
BLS签名 (https://learnblockchain.cn/tags/BLS%E7%AD%BE%E5%90%8D)

> 双线性配对特性不仅可以用于签名构造，密钥协商等，还可以实现乘法的同态隐藏和校验。这一点在零知识证明项目中应用很多。另外需要说明的是，并非基于任何椭圆曲线都可以构造配对函数，对于能有效实现双线性对的椭圆曲线，称为pairing–friendly curves，例如BLS12_381曲线。

写在前面

上一篇讲述了BLS门限签名 (https://learnblockchain.cn/article/1962)，BLS签名机制和其他签名方案相比，最大的不同或者说创新在于使用了双线性配对函数，这一点在前面几篇都提到过，本文简要说一下双线性配对函数的性质。

双线性映射定义

双线性配对（Bilinear Pairing），有时也称作双线性映射，具体翻译略有不同。双线性配对在密码学中得到广泛的应用始于2001年Boneh和Franklin使用它构造了第一个实用并且安全的基于身份加密方案IBE（IBE 可参照 https://en.wikipedia.org/wiki/Identity-based_encryption (https://en.wikipedia.org/wiki/Identity-based_encryption)）。
可以看出与BLS首次提出在同一年，不是巧合，是因为二者有共同作者--Boneh教授。

> 定义：一个双线性映射是由两个向量空间上的元素，生成第三个向量空间上一个元素之函数，并且该函数对每个参数都是线性的

若有A，B，C三个向量空间，映射e: A × B → C是一个双线性映射，则A固定，B可变时，B到C的映射是线性的，B固定，A可变时，A到C的映射也是线性的，也就是说保持双线性映射中的任意一个参数固定，另一个参数对C的映射都是线性的。

即双线性的函数有两个输入，而且对这两个输入分别满足线性。

例如矩阵乘法，数据库两张表的笛卡尔积都是双线性配对的例子。

配对函数满足:

$$e(A, B + C) = e(A, B) \cdot e(A, C)$$
$$e(A + B, C) = e(A, C) \cdot e(B, C)$$
$$e(nA, B) = e(A, nB) = e(A, B)^n$$

密码学中双线性映射

密码学中的配对用法:
有三个素数p阶群乘法循环群$G_1 \cdot G_2, G_T$，三个群存在一个映射关系(函数)$e: G_1 * G_2 \rightarrow G_T$，且满足以下性质:

双线性（Bilinearity）：对于任意的$g_1 \in G_1, g_2 \in G_2$，均有$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$成立;

非退化性（Non-degeneracy）：$\exists g_1 \in G_1, g_2 \in G_2$使得 $e(g_1, g_2) \neq 1_{G_T}$(G_T单位元)。非退化性保证了只要我们选择椭圆曲线上的非单位成员G，就能得到目标群中的非单位元

可计算性（Computability）：存在有效的算法，对于$\forall g_1 \in G_1, g_2 \in G_2$，可计算$e(g_1, g_2)$,显而易见只有这样才具有可实用性。

特殊情况下$G_1 = G_2$则称该双线性配对是对称的，否则是非对称的。另外还存在一种合数阶的双线性配对，不再详述!

关于双线性映射可以通过有限域上的超椭圆曲线上的Tate对或Weil对来构造。基于pairing密码学实现库可参考PBC (Pairing-Based Cryptography) library：https://crypto.stanford.edu/pbc/ (https://crypto.stanford.edu/pbc/)
当然也有其他库可用，不再列举。

小结

双线性配对特性不仅可以用于签名构造，密钥协商等，还可以实现乘法的同态隐藏和校验。这一点在零知识证明项目中应用很多。

另外需要说明的是，并非基于任何椭圆曲线都可以构造配对函数，对于能有效实现双线性对的椭圆曲线，称为pairing-friendly curves，例如BLS12_381曲线。

关于配对的具体实现如Kate配对实现，涉及背景知识众多，且是高等数学内容，单独说起来晦涩不易理解，好在现在都有成熟的实现库，以后有机会再讲讲配对实例的具体实现吧。

配对也不是完美的， 配对实现需要对曲线做慎重选择，加之操作复杂，运算效率有所降低，例如BLS签名验证效率就比传统的ECDSA要低，配对算法的研究就是在致力改善这一点。

关于配对，还感兴趣的可以参考:

Pairings For Beginners:
http://www.craigcostello.com.au/pairings/PairingsForBeginners.pdf

Short signatures from the Weil pairing: https://www.iacr.org/archive/asiacrypt2001/22480516.pdf (https://www.iacr.org/archive/asiacrypt2001/22480516.pdf)

既然说到了配对在零知识证明中的应用，从下一节 (https://learnblockchain.cn/article/2022)开始，我们开启零知识证明系列!
纵观区块链技术近几年的发展，密码学在区块链领域的创新应用成为区块链创新的基石与引擎，例如以太坊扩容方案zk-rollup等等。

欢迎关注公众号：blocksight

相关阅读:

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 2021-01-02 15:55 阅读（2457） 学分（6） 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)