区块链中的数学 – sigma协议OR Proof&签名

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)

本文继续讲sigma协议相关的引申和应用!

写在前面

上一篇介绍了sigma协议及非交互式范式 (https://learnblockchain.cn/article/2493)，可以看出非交互式sigma协议与之前介绍的签名机制非常相近了，如果留意他们出现的时间顺序，就会知道后者出现晚于sigma协议提出若干年后，我们相信是在此基础上发展的。

其实，任何技术（甚至“思想”）也是一样的，都是在前人基础上不断前行，站在巨人的肩膀上，才能站得高望得远!

闭门造车，向来都迫不得已才做的！所以了解目标对象的历史与现状是发展的前提。否则当你不知道一个东西的为什么出现以及在当时历史阶段所处的位置，就会有很多疑惑。

“昨夜西风凋碧树，独上高楼，望断天涯路”，说的是求知的第一阶段，即知既往，明当下。

本文继续讲sigma协议相关的引申和应用!

OR证明（OR-proof）

以指数运算为例(参数同上一篇)，假设P知晓$y_1 = g_1^{x1}$ ， $y_2 = g_2^{x2}$（mod p已省略） 等式中任意一个指数秘密，x_1或x_2者, P如何向V证明他知道其中一个但又不泄露具体哪一个呢?

前提:
g_1, g_2, g_3已公开

假设P知晓的是x_1,P流程:
1）随机选择$v_1, v_2 .w$, 计算 $t_1 = g_1^{x1}$， $t_2 = y_2^w g_2^{v2}$,

2）令c = Hash($g_1, g_2, y_1, y_2, t_1, t_2$)

3）令$c_1 = w, c_2 = c - c_1 (mod\ q)$

4）$r_1 = v_1 - c_1 x_1, r_2 = v_2 (mod\ q)$

V流程:
5） V计算$t_1' = y_1^{c1} g_1^{r1}$, $t_2' = y_2^{c1} g_2^{r2}$ 检验$t_1' =? = t_1$， $t_2' = t_2$

6） 计算 $c_1 + c_2 =? = Hash(g_1, g_2, y_1, y_2, t_1', t_2') (mod\ q)$

检验过程可自行推导!

基于Sigma协议的身份验证和签名

通过模仿Schnorr的构造，可以将任意的Sigma协议转换成身份认证方案和签名方案。假设（P,V）是构建在关系$R \subset (X * Y)$上的Sigma协议。需要添加:

1. 一个概率性(随机性)的密钥生成算法并且具有one-way特性，生成pk,sk,且（sk，pk）$\in R$
2. 安全的hash函数，作为随机Oracle，是Fiat-Shamir变换的核心

好了，完整构建的Fiat-Shamir签名方案流程如下:

1. 密钥生成算法G生成公钥（x，y）$\in R$
2. P(Prover 部分)生成承诺t， t$\in T$
3. P计算挑战 c = H(m, t)，m是待签名消息
4. P生成挑战的response z$\in Z$
5. P根据挑战z生成签名：s = (t,z)$\in T * Z$
6. V(Verifier 部分)使用公钥y,验证(t,z)$\in T * Z$,且 c = H(m, t),否则拒绝!

小结

到这里就很有意思了， 再回首看看前面介绍的签名机制（RSA，ECDSA，Schnorr,EdDSA等）,可以发现本文介绍的几乎是这些签名机制的抽象版本，他们都是具体实例化!

那么到这里签名机制就已经形成一个小的闭环，知其然知其所以然!
我们一直认为**碎片化的知识没有力量，系统化的体系才能行稳致远!**

另外基于sigma协议还有一些其他例子 如Okamoto's protocol，And proof等不再介绍!

参考:
https://zhuanlan.zhihu.com/p/144899541 (https://zhuanlan.zhihu.com/p/144899541)
https://crypto.ethz.ch/publications/files/CamSta97b.pdf

原文链接：https://mp.weixin.qq.com/s/LYgW0YVdOv4jHIh05Y0r3g
(https://mp.weixin.qq.com/s/LYgW0YVdOv4jHIh05Y0r3g)

欢迎关注公众号：blocksight

相关阅读

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

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 2021–05–11 14:54 阅读（962） 学分（1） 分类：入门/理论 (https://learnblockchain.cn/categories/basic)

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) 1856 浏览

区块链中的数学 –盲签名（Blind Signature）(https://learnblockchain.cn/article/2527) 2083 浏览

区块链中的数学 – sigma协议与Fiat–Shamir变换 (https://learnblockchain.cn/article/2493) 1589 浏览

相关问题

0 条评论

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

78 篇文章, 2219 学分

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