WEEKLY SHARING

Pinocchio Coin：简洁的，基于配对的证明系统更好构建 Zerocoin

2022.08 STEPH

ABSTRACT - 抽象的概念

背景

比特币是第一个被广泛采用的分布式电子现金系统。

Zerocoin 是最近提出的通过匿名交易扩展比特币的提议。

最初的 Zerocoin 协议在很大程度上依赖于强 RSA 假设和双离散对数证明，这是具有已知性能限制的长期技术。

我们使用椭圆曲线和双线性对展示了 Zerocoin 协议的变体。证明系统利用基于二次算术程序的现代技术，从而产生更小的证明和更快的验证。我们对 Zerocoin 的几个扩展进行了评论，这些扩展是由这些技术的通用性所支持的。

类别和主题描述

电子商务——支付方案、安全

关键词

零知识证明；匿名电子现金；比特币；零币。

RSA假设

RSA定义

RSA定义 相信只要对密码学了解的同学肯定听说过RSA，它是三个发明者名词的缩写(Rivest-Shamir-Adleman)，也是最早的公钥密码学系统之一，也是可能是应用最广泛的公钥密码学系统。这里给它两个定义

1. 广义的说，RSA密码系统(RSA cryptosystem)是基于RSA问题的公钥密码学系统
2. 狭义的说，RSA假设(RSA assumption)是一个可以构造单向陷门函数(One-way trapdoor functions)的假设。

RSA假设基于什么

保研夏令营的时候老师问我RSA假设基于啥？我其实不知道当时上课的时候说的啥，突然脑子中想起就说是基于大整数分解。老师说不对。如今仔细翻书才明白。RSA假设啥都不基于，它就是一个假设。 大整数分解如果能被解决，那么RSA一定能被解决。但是RSA被解决却不一定需要大整数分解。大整数分解是更难的问题，无法规约到RSA。

更多阅读-RSA

https://www.csdn.net/tags/MtjaIg0sNTYxNDQtYmxvZwO0O0OO0O0O.html

简介

比特币的核心组件是公共日志或交易账本。日志中的每个交易条目都将比特币金额与公钥相关联。通过检查和散列以前的交易并执行工作证明来促进日志的真实性，从而创建一个新条目；或者使用现有条目对应的私钥对新条目进行签名。后者将现有条目的比特币金额转移给新条目的公钥所有者。关于隐私，日志公开将币与其后继所有者的密钥联系起来。

ZeroCoin[MGGR13]

是一种匿名分散的电子现金系统，它既将比特币用作仅附录的公告板和储备货币。 Zerocoin使用固定的比特币量，即所有零币具有相同的面额。在不使用公共密钥，币是通过承诺代号C来匹配一对对随机生成的秘密：由币所有者保留的，非公开的S组成的序列号；公开看到R的开头序列。

为了确保匿名性，zerocoin交易涉及揭示S序列和证明R知识，为了C开头的，在之前已经大量公开收集记录到log的，承诺C0，...，CN-1中的任何C的知识。开放性的承诺，不去透露对所花费的币，而是用来计算证明π的知识签名，以取代比特币支出交易的调用签名。知识的签名证明，支出方可以打开对序列号的承诺之一，即（1）她知道c∈（c1，...，cn）和（2）C = gshr（承诺手段是佩德森承诺：它是一个涉及两方的满足完美隐藏、计算绑定的同态承诺交互协议，一般用于数据隐藏与交易验证。）。通过隐藏可以以这种方式打开的承诺，Zerocoin 提供了匿名性。同时，序列号的唯一性可防止双重 / 重复支出（double spending）。

更多阅读-佩德森承诺

https://www.jianshu.com/p/2b7a41e12626

简介

ZeroCoin[MGGR13]

使用加强的RSA，通过累加器证明C∈（C1，...，CN），因此所有承诺CI必须从间隔[A，A2）中为质量数字，以保证某些固定的Integer A，以保证两个承诺的产物不在此间隔之外。可以满足这些约束，但是基于加强的RSA的结构反而可能有它的脆弱性，因此希望拥有基于Prime-order-rorder组的替代构造。另一个并发症是由于C = GSHR是一个已经是秘密的值C和定义蓄能器的组的指数的证明。因此，这通常被称为双污物对数证明。

我们通过使用Pinocchio [PHGR13]来解决这两个问题，这是一个基于配对的新颖的证明系统，可以非常有效的进行应用。Pinocchio可以证明形式的语言l = {（ck）k∈[m‘] | e（ck）k∈[m’.. m -1]：c0 =1∧（v·c）∘（w·c）（w·c））-（y·c）= 0}，其中v，w，y是整数d，m‘，m，m，m’≤m.1p =（v，w，w，y）的d×m矩阵被称为二次算术程序（QAP）在角度D和大小M的字段F上以及决定P是否可以接受c0 = 1的p- vector（c0，cm'1）的问题，[ggpr13]显示为NP完成。

特别是语言L允许我们编码带有多个多功能门的算术电路的任意输出关系。直觉上，C编码电线值，V和W中的每一行代表电线的线性组合，该线将分别为左侧和乘法门的右输入。

简介

我们的Zerocoin的构造使用两个简单的见解：

首先，C∈（C0，...，CN -1）可以通过检查来表示算术电路i（c-ci）= 0。

第二，取而代之的是证明R的知识，我们可以证明H0的知识。 。 。 ，hν-1对于commit-enentschemesuchthat的安全参数ν，forj∈[ν]，（hj -1）（hj-h（2j））= 0 and c = s = s = gs，其中s = gs可以是公开计算。 现在，可以在[a，a2）中的素数中的素数，而是可以在离散对数问题的任何字段中定义承诺。

我们留下了一个剩下的困难。如果我们使用pinocchio的效率配对组，则在指数字段中计算指数字段fp中的离散对数相对容易。我们可以切换到非标准和较大的配对组，但这似乎是不希望的，因为它会降低证明系统的整体性能。取而代之的是，我们建议在延伸场fpμ> 2048中计算c。

我们没有声称我们的构建对于现有的强大RSA构造始终是可取的。我们方案的一个缺点是，受信任的设置而不是单个RSA模量N现在是Pinocchio QAP的评估键，一个更复杂的对象。目前尚不清楚最终在扩充场中的算术电路证明是否会比双离散对数证明更好地扩展效率。然而，一个较好证实的，显示提高了性能的特征，是验证π时，它的数据大小不再线性地取决于ν。另一个更定性的优势是基于不同的理论问题的替代构造。

构建

在介绍我们的协议时，我们假设对Zerocoin[MGGR13]和Pinocchio [PHGR13]的熟悉程度有限。

•设置（1κ）。 在输入时，安全参数，选择或生成配对友好的椭圆曲线设置G，以用于Pinocchio使用的订单P曲线。

选择随机发电机g，h∈Fpμ，使得⟨g⟩=⟨H⟩是fpμ的大乘以q |pμ-1≈2ν的大量乘法亚组。

运行评估密钥生成EK P←KEYGEN（P，G）用于PIN- OCCHIO的公开验证的零知识变体，用于验证表示为算法约束的NP关系。 对于以下证人关系，p是程度和大小o（（n +κ）μ2）的QAP，其中所有操作和值都超过fpμ：

(C0,...,Cn−1,S),(hj)κj=1 ∈ RL ⇔

∀j(hj −1)(hj −h(2j)) = 0∧i(Sj hj −Ci) = 0.

输出params =（g，p，q，g，h，ek p）作为zerocoin参数。

• Mint(params). Select a serial number and opening s,r∈Fq\1andcomputeC=gshrinFpμ.Set skc = (s, r) and output (C, skc).

• Spend(params, C, skc, C0, . . . , Cn−1). If C ∈/ (Ci)n−1 i=0

output ⊥. Compute S = gs, and hj = h2jrj, for j∈[κ],whereterj ∈{0,1}aresuchthatr= 2j rj . Then run the Pinocchio prove algorithm π ←

Compute(EKP , (C0, . . . , Cn−1, S, (h2j)ν−1), (hj)κ) and j=0 j=1

output (π, s).

• Verify(params, π, s, C0, . . . , Cn−1). Check that Verify(

EKP ,(C0, ...,Cn−1,gs,(h2j)ν−1),π) = 1. j=0

性能表现

回想一下FPμ是FP的Galois场延伸（即[P]），定义为X中多项式的FP [X]/P（X），fp中的系数在X中，fp中的系数除以p（x）=xμ-- ω，对于某些固定的ω∈FP，使P（X）是不可还原的。

We represents Elements A∈Fpμbythecoeficiations（ai）i∈[μ]，使得a（x）=iaixi。添加只是逐字化的加法：（ai）i∈[μ] +（bi）i∈[μ] =（ai + bi）i∈[μ]。乘法是μ2单词乘法的线性组合：（ai）i∈[μ] ∗（bj）j∈[μ] =（ai ∗ bj）+（ω∗ ai ∗ bj）。 k∈[μ] i+j = k i+j = k+μ

我们使用FPμ FQ。快速凸起由ν-1延长多数 用于Pedersen的承诺，有指数 plications，其中hr = 计算人力资源并证明HI的每个HI为1或H（2i）采用μ2（2ν -1）单词乘法。

Pinocchio确实在其证明的规模和证明验证成本的地方表现较好。与50KB的强RSA zerocoin 的证明数据大小，进行反差对比，Pinocchio Zerocoins的344字节的证明数据大小与现有的比特币交易支付，相当。

讨论

这只是一个非常初步的案例研究，我们还没有完整的实施或安全分析。我们的构造也没有为零协议提供的一个特征。原始的零体结构允许通过使用基于法定的Shamir的证明系统在知识的签名[CL06]模式下签署事务字符串R。从好的方面来看，我们协议的分析不再依赖于随机门。此外，我们知道扩展我们的协议的三种方法：（i）计算s作为公钥的哈希，并使用相应的秘密键签名；（ii）通过使用[HAR11]的技术构建知识的签名，使证明模拟可提取；（iii）使用基于法定的Shamir的证明系统执行部分证明，并落在随机的Oracle模型上以获得知识的签名。

我们对使用Pinocchio（例如Pinocchio）进行自定义协议设计（Pinocchio）的通用可验证计算协议的潜力感到兴奋。 Pinocchio已经允许从类似C的程序中编译算术电路。

例如，这使得通过C = HMAC（R，S）（例如基于SHA-256。也可以想象一下，更复杂的支出协议，涉及多个承诺或承诺，其平衡由类似于比特币脚本的脚本语言控制。

THANK YOU