

一种高效的范围证明方案*

张凡¹, 高胜^{1,2}, 曾志强³, 刘喆⁴

1. 兴唐通信科技有限公司, 北京 100191
2. 数据通信科学技术研究所, 北京 100191
3. 信息保障技术重点实验室, 北京 100072
4. 北京理工大学 信息和电子学院, 北京 100081

通信作者: 曾志强, E-mail: martinzeng2019@163.com

摘要: 在区块链系统中, 由于交易金额是敏感数据, 对金额的隐私保护是一个热点话题, 它不仅要求将金额隐藏, 而且需要提供该金额在某个公开范围的一个证据, 许多研究学者采用承诺方案来隐藏交易金额以及绑定该金额与对应的承诺值, 同时该承诺需要一个范围证明用来证明该金额在一个合法的区间内, 比如 $[0, 2^{64}]$. 迄今为止验证速度最快的范围证明方案是 2017 年 BÜNZ B 等人提出的 Bulletproof 方案, 该方案已广泛应用于区块链系统中. 本文在该方案的基础上通过构造新的多项式承诺方案并结合向量内积承诺方案, 提出一种高效的范围证明方案. 本文方案无需可信第三方的参与, 并且证据生成的时间复杂度约为 $(1.25n + 6.5 \log n + 4)\text{ct}$, 证据验证的时间复杂度约为 $(0.5n + 4.5 \log n + 5)\text{ct}$, 而证据的长度为 $(19 + 2 \log n)\text{cs}$, 这里 ct 表示椭圆曲线标量乘运算所需的时间, cs 表示椭圆曲线点的长度, n 为交易金额的比特长度. 与目前已知应用在区块链系统的范围证明方案相比, 本文方案在证据生成耗时、证据产生长度都相当的情况下, 将证据的验证速度达到最优, 因而是更加实用的区块链范围证明方案.

关键词: 区块链; 隐私保护; 多项式承诺; 范围证明

中图分类号: TP309.7 **文献标识码:** A **DOI:** 10.13868/j.cnki.jcr.000361

中文引用格式: 张凡, 高胜, 曾志强, 刘喆. 一种高效的范围证明方案[J]. 密码学报, 2020, 7(2): 197–211. [DOI: 10.13868/j.cnki.jcr.000361]

英文引用格式: ZHANG F, GAO S, ZENG Z Q, LIU Z. An efficient scheme of range proofs[J]. Journal of Cryptologic Research, 2020, 7(2): 197–211. [DOI: 10.13868/j.cnki.jcr.000361]

An Efficient Scheme of Range Proofs

ZHANG Fan¹, GAO Sheng^{1,2}, ZENG Zhi-Qiang³, LIU Zhe⁴

1. Xingtang Communication Technology Co. Ltd., Beijing 100191, China
2. Data Communication Science and Technology Research Institute, Beijing 100191, China
3. Science and Technology on Information Assurance Laboratory, Beijing 100072, China
4. School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China

Corresponding author: ZENG Zhi-Qiang, E-mail: martinzeng2019@163.com

Abstract: In Blockchain system, it is a hot topic for the privacy protection of the transaction amount as the sensitive data. The transaction amount should not only be hidden, but also needs a

* 基金项目: 国家重点研发计划 (2017YFB0802500)

Foundation: National Key Research and Development Program of China (2017YFB0802500)

收稿日期: 2019-04-04 定稿日期: 2019-08-23

proof which implies that the amount is in some public range. Many researchers use the commitment scheme to hide the transaction amount and bind it with the corresponding commitment. Meanwhile, the commitment scheme needs a proof to show that the amount is in a legitimate range, e.g. $[0, 2^{64})$. So far the most efficient range proof scheme with fast verification speed is the Bulletproofs scheme, which was proposed by BÜNZ B et al in 2017 and is now widely used in Blockchain systems. Based on the Bulletproofs scheme, this paper presents an efficient scheme of range proofs by combining the new construction of polynomial commitments with the vector inner-product commitments. The scheme does not need a trusted third party, and the time complexity of proof generation and proof verification are about $(1.25n + 6.5 \log n + 4)\text{ct}$ and $(0.5n + 4.5 \log n + 5)\text{ct}$ respectively, and the size of the proof is $(19 + 2 \log n)\text{cs}$, where ct represents the time complexity of the scalar multiplication of the Elliptic Curve, cs represents the size of the elements of the Elliptic Curve, and n is the binary length of the transaction amount. The time complexity of proof generation and the proof size of the proposed scheme match the current schemes of range proofs used in Blockchain systems, and the time complexity of proof verification is optimal. As a result, the scheme proposed in this paper is more suitable to provide the privacy protection in Blockchain systems.

Key words: blockchain; privacy protection; polynomial commitment; range proof

1 引言

2008 年, 化名 Satoshi Nakamoto (中本聪) 的学者在网络上发表了一篇题为《比特币: 一种点对点的电子现金系统》的文章, 于是比特币^[1]进入人们的视野. 历经十余年的发展, 各种数字货币纷纷出现, 例如门罗币^[2,3]、零币^[4]、莱特币^[5]等. 比特币具有去中心化, 分布式记账以及用户身份匿名等优点. 然而值得诟病的是, 交易金额是明文传输的, 这严重限制了比特币的广泛应用. 随后诸如门罗币和零币等数字货币采用各种密码技术 (比如环签名^[6]等特殊数字签名、承诺^[7]、零知识证明^[8]、同态加密等) 来解决交易金额的隐私保护问题. 例如门罗币采用 Borromean 环签名结合 Pedersen 承诺^[9]来实现对交易金额的隐藏, 零币则采用 zk-SNARK^[10-12]这类零知识证明对交易身份以及交易金额进行隐藏.

区块链作为数字货币的支撑技术, 本质上是采用链式数据结构来验证和存储数据并结合分布式共识机制来生成并更新数据, 从而保证全网诚实节点的状态一致性. 去中心化、可验证以及防篡改是区块链技术的基本属性. 随着对区块链技术的深入研究以及其可能的应用场景的探讨, 敏感数据的隐私保护问题显得尤为重要. 在区块链系统^[13]中, 隐私保护主要体现在两个方面: 匿名性和秘密性. 其中匿名性是指交易发起者和交易接收者的身份隐藏, 而秘密性是指交易金额的隐藏. 目前比特币系统只提供弱匿名性, 即交易发起者和交易接收者的真实身份与其对应的公钥没有关系. 门罗币和零币虽然能解决隐私保护问题, 但门罗币中证据的长度较大, 而零币需要可信任第三方的参与并且证据生成时间很长. 因而给出一个高效简洁的隐私保护方案是一个非常有挑战的问题.

为了保障交易的秘密性, Maxwell 等人提出秘密交易 (CT)^[14]概念, 即交易发起者对交易金额做承诺, 然后给出相应的证据证明该金额在某个公开的范围. Maxwell 等人利用 Borromean 环签名给出一个具体的范围证明方案, 该方案无需可信第三方的参与, 然而证据长度比较庞大并且证据生成和证据验证的时间复杂度也不小 (均与金额的比特数线性相关), 因此该方案在实际应用中很受限. Jan Camenisch 等人于 2008 年提出基于 Boneh-Boyen 签名^[15]的交互式范围证明方案^[16], 该方案后来被 Shunli Ma 等人^[17]借鉴用来保护交易金额的隐私性, 由于该方案利用双线性对并且需要可信第三方的参与, 虽然证据长度很短, 但验证时间比较长. 2017 年, Benedikt Bunz 等人^[18]提出新的范围证明方案, 该方案借鉴 Jonathan Bootle^[19]等人提出的基于多项式承诺的零知识证明方案, 并利用向量内积承诺方案将证据长度减为对数级别. 该方案不仅不需要可信第三方的参与, 而且将证据长度大大降低并且减少证据验证的时间复杂度, 这使得该方案能很好地应用在区块链系统中. 本文在 Benedikt Bunz 等人工作的基础上提出了一个新的范围证明方案, 该方案将金额按两比特划分并构造新的可满足性电路, 然后借鉴 Jonathan Bootle 等人的零知识证明方案和向量内积承诺, 将证据的生成时间和证据的验证时间大幅减少. 结合

Jonathan Bootle 等人的零知识证明方案以及向量内积承诺的安全性证明，很容易给出本文提出的范围证明方案的安全性证明。当公开区间为 $[0, 2^{64})$ 时，本文方案不仅将证据生成时间减少近一半，而且将证据验证时间减少约 33%。为了对这些范围证明方案有一个直观的认识，表1给出这四个方案的性能比较，其中 ct 表示椭圆曲线中标量点乘的时间复杂度， cs 表示椭圆曲线中点的长度。容易看出本文的范围证明方案更适合应用在区块链系统中来保护交易金额的隐私。

本文的结构如下：首先第 2 节介绍符号定义、Pedersen 承诺以及多项式承诺的基本概念。接下来第 3 节介绍 Jonathan Bootle 等人提出的对任意函数的零知识证明方案。第 4 节给出本文的范围证明方案。最后第 5 节对本文做出一个总结。

表 1 $n=64, m=8$ 具体方案性能比较

Table 1 Performance comparison among specific schemes with $n=64, m=8$

方案	证据生成时间 (ct)	证据验证时间 (ct)	证据长度 (cs)	中心
文献 [16]	89	125	26	有
文献 [14]	161	194	194	无
文献 [18]	226	94.5	21	无
本文	115	64	31	无

注：这里 n 是金额的比特长度，文献 [16] 的方案按 $m=8$ 个比特将金额分割并得到 n/m 个小块。本文假设双线性对的时间复杂度约为标量点乘的 8.5 倍。值得一提的是，文献 [20] 虽然将 CT 方案的证据生产时间和证据验证时间分别缩短了 22% 和 30%，但与本文方案相比依然有很大的差距。

2 预备知识

本节首先介绍一些符号定义，然后介绍 Pedersen 承诺、多项式承诺以及向量内积承诺等基础知识。

2.1 符号定义

下面介绍本文将要使用的符号定义。

- \mathbb{G} 满足离散对数困难问题的乘法交换群
- g 群 \mathbb{G} 的生成元
- q 群 \mathbb{G} 的阶，为大素数
- \mathbb{Z}_q 模 q 的整数环
- \mathbb{Z}_q^* 模 q 的整数环，但不包括 0 元素
- H 抵抗碰撞的哈希函数
- \circ 向量的 Hadmard 积
- \cdot 向量的内积
- \oplus 异或运算
- ct \mathbb{G} 上随机元素指数运算的计算复杂度
- ce \mathbb{G} 上双线性对运算的计算复杂度
- cs \mathbb{G} 上元素的长度

本文规定加粗的字符表示向量，未加粗的字符表示集合中的元素。并且规定 $\mathbf{g}^{\mathbf{a}} = \prod_{j=1}^n g_j^{a_j}$ ， $\mathbf{g}^x = (g_1^x, g_2^x, \dots, g_n^x)$ ，这里 $\mathbf{g} = (g_1, g_2, \dots, g_n) \in \mathbb{G}^n$ ， $\mathbf{a} = (a_1, a_2, \dots, a_n) \in \mathbb{Z}_q^n$ 。规定两个向量多项式 $\mathbf{a}(X), \mathbf{b}(X) \in \mathbb{Z}_q^n[X]$ 的乘积运算 $c(X) = \mathbf{a}(X) \cdot \mathbf{b}(X)$ 为多项式乘法并且系数之间的乘法定义为内积，此时 $c(X) \in \mathbb{Z}_q[X]$ 。

2.2 Pedersen 承诺

Pedersen 承诺^[9]是由双方参与的协议。定义公开参数 $ck = \{\mathbb{G}, q, g, h\}$ ，这里 g 是 \mathbb{G} 的生成元， $h \in \mathbb{G}$ 且其离散对数未知。

定义 1 (Pedersen 承诺) $\text{Com}_{\text{ck}}(a; r) := g^r h^a$ 为对 a 的 Pedersen 承诺, 这里 r 是随机数且不公开.

而多元 Pedersen 承诺类似于 Pedersen 承诺, 即给定公开的参数 $\text{ck} = (\mathbb{G}, q, g, h_1, \dots, h_n)$, 这里 g 是 \mathbb{G} 的生成元, $(h_1, \dots, h_n) \in \mathbb{G}^n$, 这些点的离散对数均未知. 给定消息 $(m_1, \dots, m_n) \in \mathbb{Z}_q^n$, 则对应的 Pedersen 承诺为

$$c = \text{Com}_{\text{ck}}(m_1, \dots, m_n; r) = g^r \prod_{i=1}^n h_i^{m_i}$$

Pedersen 承诺满足隐藏性 (Hiding) 和绑定性 (Binding):

隐藏性: 承诺值和随机数在计算上不可区分. 由于 r 是随机数, $C_0 = g^r h^{a_0}$ 和 $C_1 = g^r h^{a_1}$ 在计算上是不可区分的, 进而隐藏承诺内容.

绑定性: 在承诺做出之后, 承诺内容不可抵赖. 假设存在 r' 和 $a' \neq a$ 使得 $g^r h^a = C = g^{r'} h^{a'}$, 则有 $h = g^{(r-r')(a'-a)^{-1}}$, 这说明 h 的离散对数已经被求出, 而这与离散对数的困难性假设矛盾, 因此绑定性满足.

2.3 多项式承诺

假设证明者拥有多项式 $t(X) = t_0 + t_1 X + t_2 X^2 + \dots + t_{d-1} X^{d-1}$, 则该多项式承诺是一个三段式协议, 具体流程如下:

- (1) 证明者计算 $\text{pc} \leftarrow \text{PolyCommit}(t(X))$, 即对 $t(X)$ 的每个系数做承诺,

$$\text{pc} = (c_0, c_1, \dots, c_{d-1}), \text{ 其中 } c_i = \text{Com}_{\text{ck}}(t_i; r_i) = g^{r_i} h^{t_i}, i = 0, 1, \dots, d-1,$$

这里 $\text{ck} = \{\mathbb{G}, q, g, h\}$, 然后将 pc 发送给验证者.

- (2) 验证者随机选择 $x \in \mathbb{Z}_q^*$, 并将其发送给证明者.

- (3) 证明者计算 $\text{pe} \leftarrow \text{PolyEval}(x, t(X))$, 这里 $\text{pe} = (v, \rho)$, 其中 $v = t(x), \rho = \sum_{i=0}^{d-1} r_i x^i$; 并将 pe 发送给验证者.

- (4) 验证者计算 $v \leftarrow \text{PolyVerify}(\text{pc}, \text{pe}, x)$, 这里

$$v = \begin{cases} v, & \text{Com}_{\text{ck}}(v; \rho) = \prod_{i=0}^{d-1} c_i^{x^i} \\ \perp, & \text{Com}_{\text{ck}}(v; \rho) \neq \prod_{i=0}^{d-1} c_i^{x^i} \end{cases}$$

利用 Fiat-Shamir 方法, 该承诺方案变为非交互式承诺方案, 此时 $x = H(\text{pe}, \text{ck})$. 于是证明者公开承诺值 (pe, v, ρ) , 验证者则计算 x 并调用 $\text{PolyVerify}(\text{pc}, \text{pe}, x)$ 验证该承诺是否合法.

注意到承诺的长度会随多项式的次数 d 增加而线性增加. 为了降低承诺的长度, 文献 [19] 将多项式的系数分段并构造矩阵, 然后对矩阵的每一行做多元 Pedersen 承诺并构造新的多项式承诺方案, 此时承诺长度为 $O(\sqrt{d})$.

2.4 向量内积承诺

向量内积承诺是指证明者拥有两个秘密向量 $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_q^n$, 公开 $c = \mathbf{a} \cdot \mathbf{b}$ 以及 $A = g^{\mathbf{a}}$ 和 $B = h^{\mathbf{b}}$, 证明者向验证者证明 A 和 B 所蕴含的向量 \mathbf{a} 和 \mathbf{b} 之内积确实为 c .

下面介绍文献 [19] 提出的向量内积承诺方案, 不妨将该方案记做 $(\mathbb{G}, g, h, A, B, c, n; \mathbf{a}, \mathbf{b})$, 这里 g 和 h 中每个元素的离散对数互不知晓且 n 为二的幂次方.

首先将 n 维向量切成 2 个块, 每个块是 $n/2$ 维的向量, 记

$$\mathbf{g} = (g_1, g_2), \quad \mathbf{h} = (h_1, h_2), \quad \mathbf{a} = (a_1, a_2), \quad \mathbf{b} = (b_1, b_2)$$

这里 $g_1, g_2, h_1, h_2 \in \mathbb{G}^{n/2}, a_1, a_2, b_1, b_2 \in \mathbb{Z}_q^{n/2}$, 则

$$A = g_1^{a_1} g_2^{a_2}, \quad B = h_1^{b_1} h_2^{b_2}, \quad c = a \cdot b = a_1 \cdot b_1 + a_2 \cdot b_2$$

然后令 $a'(X) = a_1 X + a_2 X^2, b'(X) = b_1 X^{-1} + b_2 X^{-2}$, 于是 $a'(X) \cdot b'(X)$ 的常数项等于 c . 设随机数 $x \in \mathbb{Z}_q^*$, 令 $a' = a'(x), b' = b'(x)$ 以及 $g' = g_1^{x^{-1}} \circ g_2^{x^{-2}}, h' = h_1^x \circ h_2^{x^2}$, 则

$$\begin{aligned} (g')^{a'} &= A_{-1}^{x^{-1}} A_0 A_1^x, \quad \text{这里 } A_{-1} = g_2^{a_1}, A_0 = g_1^{a_1} g_2^{a_2}, A_1 = g_1^{a_2}, \\ (h')^{b'} &= B_{-1}^{x^{-1}} B_0 B_1^x, \quad \text{这里 } B_{-1} = h_1^{b_2}, B_0 = h_1^{b_1} h_2^{b_2}, B_1 = h_2^{b_1}, \\ c' &= a' \cdot b' = c_{-1} x^{-1} + c_0 + c_1 x, \quad \text{这里 } c_{-1} = a_1 \cdot b_2, c_0 = a_1 \cdot b_2 + a_1 \cdot b_2, c_1 = a_2 \cdot b_1 \end{aligned}$$

如果令 $A' = (g')^{a'}, B' = (h')^{b'}$, 则原向量内积承诺转化为对新向量 a' 和 b' 的内积承诺. 注意到验证者需要计算 g', h', A', B' 以及 c' , 证明者需要传输 A_k, B_k 和 c_k , 这里 $k \in \{-1, 1\}$.

下面描述该向量内积承诺方案 $(\mathbb{G}, g, h, A, B, c, n; a, b)$ 的具体过程, 这里只有 a 和 b 是秘密. 在下面的过程描述中, P 是指证明者, 而 V 是指验证者.

公开输入: $g, h \in \mathbb{G}^n, A, B \in \mathbb{G}, c \in \mathbb{Z}_q^*$, 并且假设 n 为二的幂次方.

秘密输入: 证明者拥有 (a, b) 且满足 $A = g^a, B = h^b$ 以及 $c = a \cdot b$.

协议过程: (1) 当 $(n > 1)$ 时, 执行递归约减步骤:

- $P \rightarrow V$: 发送 $A_{-1}, B_{-1}, c_{-1}, A_1, B_1, c_1$ 共 6 个元素 (注意到 $A_0 = A, B_0 = B$ 和 $c_0 = c$, 这三元组不用发送);
- $P \leftarrow V$: 发送随机数 $x \in \mathbb{Z}_q^*$;
- $P \rightarrow V$: P 和 V 分别将原始知识证明问题转化为如下知识证明问题

$$(\mathbb{G}, g', h', A', B', c', n/2; a', b')$$

这里

$$\begin{aligned} g' &= g_1^{x^{-1}} \circ g_2^{x^{-2}}, \quad A' = A_{-1}^{x^{-1}} A_0 A_1^x \\ h' &= h_1^x \circ h_2^{x^2}, \quad B' = B_{-1}^{x^{-1}} B_0 B_1^x \\ c' &= c_{-1} x^{-1} + c_0 + c_1 x \end{aligned}$$

此外, P 还需更新自己的秘密输入, 即 $a' = a_1 x + a_2 x^2$ 和 $b' = b_1 x^{-1} + b_2 x^{-2}$.

然后 P 和 V 循环执行该递归约减步骤.

(2) 当 $(n = 1)$ 时, 执行终止步骤:

- $P \rightarrow V$: P 直接发送 (a, b) ;
- $P \leftarrow V$: 如果 $A = g^a, B = h^b$ 以及 $c = ab$ 成立, 则返回接受, 否则拒绝.

上述方案中证明者需要向验证者发送 A_i, B_i 以及 c_i , 所需的通信带宽较大. 为了降低通信复杂度, 文献 [18] 考虑 $P = g^a h^b g_t^c$, 这里 $c = a \cdot b, g_t$ 的离散对数未知. 此时在递归约减的步骤中 A_i, B_i 和 c_i 可以合并发送. 不妨将该承诺方案记做 $(\mathbb{G}, g_t, g, h, P, n; a, b)$, 下面是其具体过程.

公开输入: $g, h \in \mathbb{G}^n, g_t, P \in \mathbb{G}$, 这里 n 是二的幂次方.

秘密输入: 证明者拥有 $a = (a_1, a_2), b = (b_1, b_2)$ 并满足 $P = g_1^{a_1} g_2^{a_2} h_1^{b_1} h_2^{b_2} g_t^c$, 这里

$$g = (g_1, g_2), \quad h = (h_1, h_2), \quad c = a_1 \cdot b_1 + a_2 \cdot b_2$$

协议过程: 如果 $n = 1$, 则

- $P \rightarrow V$: 直接发送 (a, b)
- $P \leftarrow V$: 如果 $P = g^a h^b g_t^c$, 这里 $c = ab$, 则返回接受; 否则拒绝.

递归约减: 如果 $n > 1$, 则证明者令 $n' = n/2$, 然后计算

- $P \rightarrow V$: 发送 (L, R) , 这里 $L = g_2^{a_1} h_1^{b_2} g_t^{c_L}$, $c_L = a_1 \cdot b_2 \in \mathbb{Z}_q$, $R = g_1^{a_2} h_2^{b_1} g_t^{c_R}$,
 $c_R = a_2 \cdot b_1 \in \mathbb{Z}_q$.
- $P \leftarrow V$: 发送随机数 $x \in \mathbb{Z}_q^*$
- 证明者和验证者将原问题转化为如下新问题

$$(\mathbb{G}, g_t, g', h', P', n'; a', b')$$

这里

$$g' = g_1^{x^{-1}} \circ g_2^{x^{-2}}, \quad h' = h_1^x \circ h_2^{x^2}, \quad P' = L^{x^{-1}} P R^x$$

而且证明者还需计算

$$a' = a_1 x + a_2 x^2 \in \mathbb{Z}_q^{n'}, \quad b' = b_1 x^{-1} + b_2 x^{-2} \in \mathbb{Z}_q^{n'}$$

综上, 第一个向量内积承诺方案的通信复杂度为 $6 \log n + 2$, 而第二个向量内积承诺方案的通信复杂度为 $2 \log n + 2$, 而且第二个方案的计算复杂度比第一个方案小. 引理 1 给出这两个内积承诺方案的安全性.

引理 1 上述向量内积承诺方案具有完美完全性 (perfect completeness) 和统计的见证扩展仿真性 (statistical witness-extended-emulation), 即提取出非平凡的离散对数或者提出有效的见证 (witness).

证明请参考文献 [18].

3 算术电路的无中心零知识证明方案

零知识证明由 Goldwasser 等人^[21]于上世纪 80 年代提出. 它是一种密码学技术, 通过交互, 证明者向验证者证明某个提议是正确的并且无需泄露除了它是正确之外的任何信息. 后来, Goldreich 等人^[22]证明任何 NP 问题都有零知识证明系统. 至此人们提出许多零知识证明方案, 其中最为著名的是 Fiat-Shamir 零知识身份认证协议^[23-25], 其安全性建立在大整数分解问题的困难性, 然而其通信和计算复杂度太大, 因而实用性不强. 2013 年, Parno 等人提出匹诺曹协议^[10], 该协议是一个简洁非交互式零知识证明协议 (zk-SNARK), 并且用于对任意布尔 (或算术) 电路的可信计算. 该协议最大的优势是无论可满足性电路有多复杂, 其证据的长度固定为 288 字节. 2016 年, Bootle 等人^[19]提出另外一种零知识证明协议, 该协议同样用于对任意布尔电路的可信计算. 与匹诺曹协议不同的是, 该协议不仅无需可信第三方以及复杂的预计算过程, 而且其安全性只依赖于离散对数的困难性. 2017 年, Bootle 等人^[26]提出可以批处理的零知识证明, 该方法将多个秘密满足的简单电路转化为低次数的多项式, 进而利用多项式承诺给出高效的证明. 2018 年, Wahby 等人^[27]提出新的 zk-SNARK 协议 Hyrax, 该协议结合 Pedersen 承诺、求和验证协议等密码学工具对任意电路实现可信计算, 并且无需可信第三方以及安全性假设只依赖于离散对数问题. 除此之外, Huige WANG 等人^[28,29]借鉴这类对可满足性电路的零知识证明方法并应用在功能加密和访问控制加密中.

本节介绍 Bootle 等人的零知识证明方案, 其中 3.1 节介绍算术电路转化为代数表达式的过程, 第 3.2 节介绍代数表达式转化为向量多项式的过程, 接下来 3.3 节介绍基于多项式承诺的零知识证明方案, 最后 3.4

节给出该零知识证明方案的具体过程.

3.1 算术电路的代数表达式刻画

本节介绍将任意给定算术电路转化为代数表达式的过程.

如图1所示, 首先对每个乘法门分配相应的 (a_i, b_i, c_i) , 其对应的代数表达式为 $a_i b_i = c_i$; 其次对于常数乘法门以及异或门, 利用相关输入输出的仿射表达式刻画, 例如图1中右侧的线性表达式给出了常数乘法门和异或门的代数刻画.

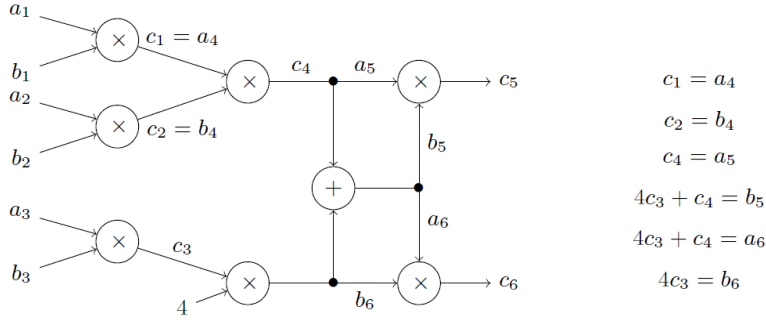


图1 算术电路的代数表达式刻画

Figure 1 Algebraic expression of arithmetic circuit

假设该电路图的乘法门个数 $N = m * n$, (a_i, b_i, c_i) 则用三个 $m * n$ 的矩阵 (A, B, C) 表示, 定义 $A \circ B = C$, 这里 A, B 和 C 的每一行表示为

$$a_i = (a_{i,1}, \dots, a_{i,n}), \quad b_i = (b_{i,1}, \dots, b_{i,n}), \quad c_i = (c_{i,1}, \dots, c_{i,n})$$

且满足 $a_i \circ b_i = c_i$, 其中 $i \in \{1, \dots, m\}$. 每个仿射表达式的刻画表示如下

$$\sum_{i=1}^m a_i \cdot w_{q,a,i} + \sum_{i=1}^m b_i \cdot w_{q,b,i} + \sum_{i=1}^m c_i \cdot w_{q,c,i} = K_q, \quad q \in \{1, \dots, Q\}$$

这里 $w_{q,a,i}, w_{q,b,i}, w_{q,c,i}$ 和 K_q 是只与电路有关的常数, Q 是仿射表达式的个数.

3.2 算术电路的多项式转化

本节介绍将代数表达式转化为单变元多项式的过程. 设 Y 是自变量, 定义 $Y' = (Y^m, Y^{2m}, \dots, Y^{nm})$ 和 $Y = (Y, Y^2, \dots, Y^m)$, 则 $Y(A \circ B)Y'^T = YCY'^T$, 展开得

$$\sum_{i=1}^m (a_i \cdot (b_i \circ Y')) Y^i = \sum_{i=1}^m (c_i \cdot Y') Y^i$$

即 Y^{i+jm} 对应的系数满足 $a_{i,j} b_{i,j} = c_{i,j}$. 令 $M = N + m$, 对于 Q 个仿射表达式, 则有

$$\sum_{q=1}^Q \left(\sum_{i=1}^m a_i \cdot w_{q,a,i} + b_i \cdot w_{q,b,i} + c_i \cdot w_{q,c,i} \right) Y^q = \sum_{q=1}^Q K_q Y^q$$

将上面的两个表达式联立, 有

$$\left(\sum_{i=1}^m (a_i \cdot (b_i \circ Y')) Y^i \right) + \sum_{i=1}^m a_i \cdot \left(\sum_{q=1}^Q w_{q,a,i} Y^{M+q} \right) + \sum_{i=1}^m b_i \cdot \left(\sum_{q=1}^Q w_{q,b,i} Y^{M+q} \right) +$$

$$\sum_{i=1}^m c_i \cdot \left(-Y^i Y' + \sum_{q=1}^Q w_{q,c,i} Y^{M+q} \right) = \sum_{q=1}^Q K_q Y^{M+q}$$

定义

$$\begin{aligned} w_{a,i}(Y) &= \sum_{q=1}^Q w_{q,a,i} Y^{M+q}, & w_{b,i}(Y) &= \sum_{q=1}^Q w_{q,b,i} Y^{M+q} \\ w_{c,i}(Y) &= -Y^i Y' + \sum_{q=1}^Q w_{q,c,i} Y^{M+q}, & K(Y) &= \sum_{q=1}^Q K_q Y^{M+q} \end{aligned}$$

于是电路是可满足的当且仅当

$$\sum_{i=1}^m (a_i \cdot (b_i \circ Y')) Y^i + \sum_{i=1}^m a_i \cdot w_{a,i}(Y) + \sum_{i=1}^m b_i \cdot w_{b,i}(Y) + \sum_{i=1}^m c_i \cdot w_{c,i}(Y) - K(Y) = 0$$

设验证者发送随机数 $y \in \mathbb{Z}_q^*$, 此时证明者需要证明

$$\sum_{i=1}^m (a_i \cdot (b_i \circ y')) y^i + \sum_{i=1}^m a_i \cdot w_{a,i}(y) + \sum_{i=1}^m b_i \cdot w_{b,i}(y) + \sum_{i=1}^m c_i \cdot w_{c,i}(y) - K(y) = 0$$

这里 $y' = (y^m, y^{2m}, \dots, y^{nm})$.

3.3 基于多项式承诺的零知识证明

根据算术电路的代数表达式刻画, 证明者构造如下洛朗多项式:

$$\begin{aligned} r(X) &:= \sum_{i=1}^m a_i y^i X^i + \sum_{i=1}^m b_i X^{-i} + X^m \sum_{i=1}^m c_i X^i + d X^{2m+1} \\ s(X) &:= \sum_{i=1}^m w_{a,i} y^{-i} X^{-i} + \sum_{i=1}^m w_{b,i} X^i + X^{-m} \sum_{i=1}^m w_{c,i} X^{-i} \\ r'(X) &:= r(X) \circ y' + 2s(X) \\ t(X) &:= r(X) \cdot r'(X) - 2K(y) \end{aligned}$$

这里 d 为盲化向量. 容易验证 $t(X)$ 的常数项为零.

一种非常直接的思路是, 证明者首先将 a_i, b_i, c_i 和 d 的承诺发送给验证者, 随后验证者随机选取 $y \in \mathbb{Z}_q^*$ 并将其发送给证明者, 接下来证明者利用 PolyCommit 将 $t(X)$ 的承诺 pc 发送给验证者, 验证者随后随机选取 $x \in \mathbb{Z}_q^*$ 并将其发送给证明者, 然后证明者将 $r(x)$ 以及由 PolyEval 产生的 pe 一并发送给验证者, 此时验证者首先根据 a_i, b_i, c_i 和 d 的承诺验证 $r(x)$ 的正确性, 然后计算 $s(x)$ 和 $K(y)$ 以及 $r'(x)$, 接着验证者根据 (pc, pe) 验证承诺的正确性并计算 $t(X)$ 在 x 处的取值, 最后验证者判断 $t(x) \stackrel{?}{=} r(x) \cdot r'(x) - 2K(y)$ 是否成立即确定该证据是否为对应电路的合法零知识证明.

文献 [18] 的作者利用向量内积承诺给出更高效的证明方案. 注意到

$$g^r = \text{Com}_{\text{ck}}(0; -\rho) \prod_{i=1}^m A_i^{x^i y^i} \prod_{i=1}^m B_i^{x^{-i}} \prod_{i=1}^m C_i^{x^{m+i}} D^{x^{2m+1}}$$

这里 A_i, B_i, C_i 和 D 分别是 a_i, b_i, c_i 和 d 的承诺, 即

$$A_i = \text{Com}_{\text{ck}}(a_i, \alpha_i), \quad B_i = \text{Com}_{\text{ck}}(b_i, \beta_i), \quad C_i = \text{Com}_{\text{ck}}(c_i, \gamma_i), \quad D = \text{Com}_{\text{ck}}(d, \delta)$$

其中 $\text{ck} = \{\mathbb{G}, q, g, \mathbf{g} = (g_1, g_2, \dots, g_n)\}$. 如果令 $\mathbf{h} = (g_1^{y^{-m}}, \dots, g_n^{y^{-nm}})$, 则 $\mathbf{g}^r = \mathbf{h}^{r \circ \mathbf{y}'}$ 并且 $\mathbf{h}^{r'} = \mathbf{g}^r \mathbf{h}^{2s}$. 设 $v = t(x)$, 则 $\mathbf{r} \cdot \mathbf{r}' = v + 2K(y)$. 此时该零知识证明方案转化为如下向量内积承诺方案

$$(\mathbb{G}, \mathbf{g}, \mathbf{h}, R, R', v + 2K(y), n; \mathbf{r}, \mathbf{r}')$$

这里 $R = \mathbf{g}^r, R' = R * \mathbf{h}^{2s} = \mathbf{h}^{r'}$, 此时证明者的秘密输入是 \mathbf{r} 和 \mathbf{r}' , 而验证者通过多项式承诺方案得到 v 的取值.

3.4 零知识证明方案的具体描述

本小节介绍零知识证明方案的详细过程, 其中 P 是指证明者, V 是指验证者.

公开输入: $(\text{ck}, \mathcal{C}, N, m, n)$, 这里 $\text{ck} = (\mathbb{G}, q, g, \mathbf{g}), \mathbf{g} = (g_1, g_2, \dots, g_n) \in \mathbb{G}^n$ 和函数 f 的布尔电路 \mathcal{C} .

秘密输入: P 拥有 $\{(\mathbf{a}_i, \mathbf{b}_i, \mathbf{c}_i)\}_{i=1}^N$, 使得其满足函数 f 对应的布尔电路 \mathcal{C} .

证明阶段:

- $P \rightarrow V$: 随机选择 $\alpha_1, \beta_1, \gamma_1, \dots, \alpha_m, \beta_m, \gamma_m, \delta \leftarrow \mathbb{Z}_q^n$ 以及盲化向量 $\mathbf{d} \leftarrow \mathbb{Z}_q^n$, 计算

$$A_i = \text{Com}_{\text{ck}}(\mathbf{a}_i; \alpha_i), B_i = \text{Com}_{\text{ck}}(\mathbf{b}_i; \beta_i), C_i = \text{Com}_{\text{ck}}(\mathbf{c}_i; \gamma_i), D = \text{Com}_{\text{ck}}(\mathbf{d}; \delta)$$

然后将 $A_1, B_1, C_1, \dots, A_m, B_m, C_m, D$ 发送给 V .

- $P \leftarrow V$: 随机选择 $y \in \mathbb{Z}_q^*$ 并将其发送给 P , 然后 P 和 V 均计算

$$K = K(y), \mathbf{w}_{a,i} = \mathbf{w}_{a,i}(y), \mathbf{w}_{b,i} = \mathbf{w}_{b,i}(y) \text{ 和 } \mathbf{w}_{c,i} = \mathbf{w}_{c,i}(y)$$

- $P \rightarrow V$: 计算洛朗多项式

$$\begin{aligned} \mathbf{r}(X) &:= \sum_{i=1}^m \mathbf{a}_i y^i X^i + \sum_{i=1}^m \mathbf{b}_i X^{-i} + X^m \sum_{i=1}^m \mathbf{c}_i X^i + \mathbf{d} X^{2m+1} \\ \mathbf{s}(X) &:= \sum_{i=1}^m \mathbf{w}_{a,i} y^{-i} X^{-i} + \sum_{i=1}^m \mathbf{w}_{b,i} X^i + X^{-m} \sum_{i=1}^m \mathbf{w}_{c,i} X^{-i} \\ \mathbf{r}'(X) &:= \mathbf{r}(X) \circ \mathbf{y}' + 2\mathbf{s}(X) \\ t(X) &:= \mathbf{r}(X) \cdot \mathbf{r}'(X) - 2K(y) \end{aligned}$$

然后对 $t(X)$ 做承诺, 即 $\text{pc} \leftarrow \text{PolyCommit}(t(X))$, 并将 pc 发给 V .

- $P \leftarrow V$: 发送随机数 $x \in \mathbb{Z}_q^*$
- $P \rightarrow V$: 计算 $\text{pe} \leftarrow \text{PolyEval}(x, t(X))$ 以及

$$\begin{aligned} \mathbf{r} &= \sum_{i=1}^m \mathbf{a}_i y^i x^i + \sum_{i=1}^m \mathbf{b}_i x^{-i} + x^m \sum_{i=1}^m \mathbf{c}_i x^i + \mathbf{d} x^{2m+1}, \\ \rho &= \sum_{i=1}^m \alpha_i y^i x^i + \sum_{i=1}^m \beta_i x^{-i} + x^m \sum_{i=1}^m \gamma_i x^i + \delta x^{2m+1} \end{aligned}$$

如果 $n = 1$, 将 $(\text{pe}, \mathbf{r}, \rho)$ 发送给 V ;

否则计算 $\mathbf{r}' = \mathbf{r} \circ \mathbf{y}' + 2\mathbf{s}(x)$, 并将 (pe, ρ) 发送给 V .

验证阶段: 首先 V 计算 $v \leftarrow \text{PolyVerify}(\text{pc}, \text{pe}, x)$, 如果 $v = \perp$ 则拒绝并验证失败.

- 如果 $n = 1$, V 根据收到的 \mathbf{r} 计算 $\mathbf{r}' = \mathbf{r} \circ \mathbf{y}' + 2\mathbf{s}(x)$ 并且验证

$$\mathbf{r} \cdot \mathbf{r}' = 2K + v$$

$$\text{Com}_{\text{ck}}(\mathbf{r}; \rho) = \prod_{i=1}^m A_i^{x^i y^i} \prod_{i=1}^m B_i^{x^{-i}} \prod_{i=1}^m C_i^{x^{m+i}} D^{x^{2m+1}}$$

- 如果 $n > 1$, P 和 V 运行如下向量内积承诺

$$(\mathbb{G}, \mathbf{g}, \mathbf{h}, R, R', v + 2K, n/2; \mathbf{r}, \mathbf{r}')$$

这里

$$\mathbf{g} = (g_1, g_2, \dots, g_n), \quad \mathbf{h} = (g_1^{y^{-m}}, g_2^{y^{-2m}}, \dots, g_n^{y^{-nm}})$$

$$R = \text{Com}_{\text{ck}}(0; -\rho) \prod_{i=1}^m A_i^{x^i y^i} \prod_{i=1}^m B_i^{x^{-i}} \prod_{i=1}^m C_i^{x^{m+i}} D^{x^{2m+1}} = \mathbf{g}^{\mathbf{r}}$$

$$R' = R \cdot \mathbf{h}^{2\mathbf{s}} = \mathbf{h}^{\mathbf{r}'}$$

引理 2 给出上述对任意可满足性电路的基于多项式承诺的零知识证明方案的安全性。

引理 2 上述对可满足性电路的零知识证明方案满足完美完全性 (perfect completeness)、完美诚实验证者零知识性 (perfect special honest verifier zero-knowledge) 以及统计的见证扩展模拟性 (statistical witness-extended emulation), 即提取一个违背承诺方案绑定性的实例或者可满足性电路中的见证 (witness)。

证明请参考文献 [19]。

4 高效的范围证明方案

范围证明是零知识证明在区块链系统中的一个重要应用。范围证明是指对于某个值 $v \in [0, 2^n)$, 证明者构造 Pedersen 承诺 $V = g^w h^v$ 以及相应的证据, 以证明该值 v 确实在范围 $[0, 2^n)$ 中。

文献 [18] 将 v 按单比特处理, 即令 $v = \sum_{i=0}^{n-1} v_i * 2^i$, 则 $v_i(v_i - 1) = 0$, 根据这两个方程构造多项式, 并利用多项式承诺构造范围证明。最后他们提出的改进的向量内积承诺将证据的长度减为 $O(\log n)$ 。本文将 v 按两比特处理并构造新的多项式, 然后构造相应的多项式承诺, 最后结合向量内积承诺给出高效的范围证明方案。

4.1 新方案描述

令 $v = \sum_{i=0}^{k-1} v_i 4^i$, 这里 $k = n/2$ 。此时 $v_i(v_i - 1)(v_i - 2)(v_i - 3) = 0$ 。令

$$\mathbf{a} = (v_0, v_1, \dots, v_{k-1}),$$

$$\mathbf{b} = \mathbf{a} - \mathbf{3}, \mathbf{c} = \mathbf{a} \circ \mathbf{b}, \mathbf{d} = \mathbf{c} + \mathbf{2},$$

$$v = \mathbf{a} \cdot \mathbf{t}_4$$

这里定义

$$\mathbf{3} = \underbrace{3, \dots, 3}_k, \mathbf{2} = \underbrace{2, \dots, 2}_k, \mathbf{t}_4 = (1, 4, \dots, 4^{k-1}) \in \mathbb{Z}_q^k$$

按照前面介绍的方法, 我们构造两个洛朗多项式 $\mathbf{r}(X)$ 和 $\mathbf{r}'(X)$, 使得这两个向量多项式的乘积多项式的常数项为零, 即令

$$\mathbf{r}(X) = \mathbf{a}y^{-1}X + \mathbf{b}X^{-1} + \mathbf{c}X^2 + \mathbf{d}X^{-2} + \mathbf{c}y^{-1}X^3 + \mathbf{e}X^4$$

$$\begin{aligned}
s(X) &= \mathbf{y} \cdot y^{2k} \cdot (yX^{-1} - X + y^k X^{-2} - y^k X^2) + t_4 y X^{-1} - 2\mathbf{y}' X^{-3} \\
\mathbf{r}'(X) &= \mathbf{r}(X) \circ \mathbf{y}' + s(X) \\
t(X) &= \mathbf{r}(X) \cdot \mathbf{r}'(X) - K(y)
\end{aligned}$$

这里 $\mathbf{y} = (y, y^2, \dots, y^k) \in \mathbb{Z}_q^k$, $\mathbf{y}' = (y^2, y^4, \dots, y^{2k}) \in \mathbb{Z}_q^k$ 以及 $K(y) = y^{2k} \cdot \mathbf{y} \cdot (\mathbf{3} + 2\mathbf{y}^k)$. 于是 $t(X)$ 的常数项

$$\begin{aligned}
t_0 &= 2(\mathbf{a} \circ \mathbf{b} - \mathbf{c}) \cdot \mathbf{y}' \cdot y^{-1} + 2(\mathbf{c} \circ \mathbf{d}) \cdot \mathbf{y}' + \mathbf{y} \cdot y^{2k}((\mathbf{a} - \mathbf{b}) + (\mathbf{c} - \mathbf{d}) \cdot y^k) + (\mathbf{a} \cdot t_4) - K(y) \\
&= y^{2k} \cdot \mathbf{y} \cdot (\mathbf{3} + 2\mathbf{y}^k) + v - K(y) = v
\end{aligned}$$

在介绍协议的执行过程之前, 令该协议的公开参数 $(\mathbb{G}, q, g, h, g_s, h_s, g_u, \mathbf{g}, \mathbf{h})$, 这里 $\mathbf{g} = (g_1, g_2, \dots, g_k)$, $\mathbf{h} = (h_1, h_2, \dots, h_k)$, 且 $\mathbf{g}, \mathbf{h}, g, h, g_s, h_s, g_u$ 的离散对数互不知晓. 下文的过程描述中 P 是指证明者, V 是指验证者.

证明过程:

- P \rightarrow V: 随机选择 $\alpha, \beta, \gamma, \delta, \theta \in \mathbb{Z}_q^*$ 以及盲化向量 $\mathbf{e} \in \mathbb{Z}_q^{*k}$, 计算

$$\begin{aligned}
A &= \text{Com}_{\text{ck}}(\mathbf{a}; \alpha), B = \text{Com}_{\text{ck}}(\mathbf{b}; \beta), C = \text{Com}_{\text{ck}}(\mathbf{c}; \gamma), \\
D &= \text{Com}_{\text{ck}}(\mathbf{d}; \delta), E = \text{Com}_{\text{ck}}(\mathbf{e}; \theta)
\end{aligned}$$

这里 $\text{ck} = \{\mathbb{G}, q, g, \mathbf{g}\}$, 然后将 A, B, C, D 和 E 发送给验证者.

- P \leftarrow V: 发送随机值 $y \in \mathbb{Z}_q^*$, 然后 P 计算 $s(X)$ 和 $K(y)$
- P \rightarrow V: P 计算洛朗多项式

$$\begin{aligned}
\mathbf{r}(X) &= \mathbf{a}y^{-1}X + \mathbf{b}X^{-1} + \mathbf{c}X^2 + \mathbf{d}X^{-2} + \mathbf{c}y^{-1}X^3 + \mathbf{e}X^4 \\
s(X) &= \mathbf{y} \cdot y^{2k} \cdot (yX^{-1} - X + y^k X^{-2} - y^k X^2) + t_4 y X^{-1} - 2\mathbf{y}' X^{-3} \\
\mathbf{r}'(X) &= \mathbf{r}(X) \circ \mathbf{y}' + s(X) \\
t(X) &= \mathbf{r}(X) \cdot \mathbf{r}'(X) - K(y)
\end{aligned}$$

然后对 $t(X)$ 的非零系数做承诺, 即 $T_i = g_s^{\tau_i} h_s^{t_i}$, 这里 $t(X) = \sum_{i=-5}^6 t_i X^i$, $i \in \{-5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6\}$. P 将这 11 个承诺值发送给 V.

- P \leftarrow V: 发送随机值 $x \in \mathbb{Z}_q^*$, V 计算

$$s = s(x) = \mathbf{y} \cdot y^{2k} (yx^{-1} - x + y^k x^{-2} - y^k x^2) + t_4 y x^{-1} - 2\mathbf{y}' x^{-3}$$

- P \rightarrow V: P 计算

$$\begin{aligned}
\mathbf{r} &= \mathbf{r}(x) = \mathbf{a}y^{-1}x + \mathbf{b}x^{-1} + \mathbf{c}x^2 + \mathbf{d}x^{-2} + \mathbf{c}y^{-1}x^3 + \mathbf{e}x^4 \\
\rho &= \alpha y^{-1}x + \beta x^{-1} + \gamma x^2 + \delta x^{-2} + \gamma y^{-1}x^3 + \theta x^4 \\
s &= s(x) = \mathbf{y} \cdot y^{2k} \cdot (yx^{-1} - x + y^k x^{-2} - y^k x^2) + t_4 y x^{-1} - 2\mathbf{y}' x^{-3}
\end{aligned}$$

以及 $t = t(x) = \mathbf{r} \cdot (\mathbf{r} \circ \mathbf{y}' + s)$ 和 $\tau_x = \sum_{i=-5}^6 \tau_i x^i$, 这里 $\tau_0 = \omega$, 即承诺值 V 的随机指数. 如果 $k = 1$, P 将 τ_x, ρ, \mathbf{r} 发送给 V; 否则 P 将 τ_x, ρ, t 发给 V.

验证过程: 首先验证者根据收到的 τ_x 和 t 验证 $g_s^{\tau_x} h_s^t = V \cdot \prod_{i=-5}^6 T_i^{x^i}$ 是否成立, 如果不成立, 则验证失败. 其次,

- 如果 $k = 1$, V 根据 r 计算 $t = r \cdot (r \circ y' + s) - K(y)$ 并验证

$$\text{Com}_{\text{ck}}(r; \rho) = A^{y^{-1}x} B^{x^{-1}} C^{x^2} D^{x^{-2}} C^{y^{-1}x^3} E^{x^4}$$

是否成立, 如果不成立, 则验证失败.

- 如果 $k > 1$, P 和 V 均计算 $R = A^{y^{-1}x} B^{x^{-1}} C^{x^2} D^{x^{-2}} C^{y^{-1}x^3} E^{x^4} g^{-\rho} = g^r$ 并计算

$$h_v := (h_1^{y^{-2}}, h_2^{y^{-4}}, \dots, h_k^{y^{-2k}}) \text{ 和 } g_v = (g_1/h_1, g_2/h_2, \dots, g_k/h_k)$$

然后计算 $R' = R \cdot h_v^s g_u^{t+K(y)} = g_v^r h_v^{s'} g_u^{t+K(y)}$. 接下来 P 和 V 运行如下向量内积承诺

$$(\mathbb{G}, q, g_u, g_v, h_v, R', k; r, r')$$

本节给出的范围证明方案是交互式方案, 为了将其应用在区块链系统中, 利用 Fiat-Shamir 变换很容易将其变为非交互式范围证明方案.

定理 1 本文提出的范围证明方案具有完美完整性 (perfect completeness)、完美诚实验证者零知识性 (perfect honest verifier zero-knowledge) 以及计算特殊合理性 (computational special soundness).

证明: 证明者和验证者在运行向量内积承诺之前, 他们的交互过程与文献 [19] 中的对可满足性电路的零知识证明方案的过程一致. 如果证明者和验证者不运行向量内积承诺, 而是证明者在最后一步将 $t(X)$ 的承诺以及 r 直接发送给验证者, 根据引理 1 和多项式承诺的完美完整性和统计特殊合理性 (statistical special soundness), 该修改的范围证明方案具有完美完整性、完美诚实验证者零知识性以及计算特殊合理性. 而本文提出的范围证明方案是将向量内积承诺替换这个修改范围证明方案的最后一步, 由于 g_u, g, h 的离散对数互不知晓, 根据引理 2 以及类似文献 [18] 对计算特殊合理性的证明, 本文提出的范围证明方案具有完美完整性、完美诚实验证者零知识性以及计算特殊合理性. \square

4.2 新方案性能分析

本文我们只考虑将 \mathbb{G} 上的指数运算作为对范围证明方案的计算复杂度的估计, 这是因为 \mathbb{Z}_q 上的算术运算与 \mathbb{G} 上的指数运算相比可以忽略不计. 记 ct 为 \mathbb{G} 上随机元素的指数运算所需的时间复杂度, 指数运算由平方和乘法运算组成. 本文假设指数运算所需的总平方运算和总乘法运算耗时相当, 并且假设固定元素的指数运算所需要的时间复杂度只占随机元素指数运算时间复杂度的一半 (这里暂不考虑建表等优化细节). 设 cs 为 \mathbb{G} 上元素的长度并且假设 \mathbb{G} 中元素和 \mathbb{Z}_q 中元素的比特长度相同 (如果考虑 \mathbb{G} 为椭圆曲线群, 利用点压缩技术后, \mathbb{G} 中元素只比 \mathbb{Z}_q 中元素多 1 比特).

下面分析本文方案的计算复杂度和证据长度. 在运行内积向量承诺 $(\mathbb{G}, q, g_u, g_v, h_v, R', k; r, r')$ 之前, 证明者的计算开销主要是 (A, B, C, D, E) 的计算、11 个 T_i 的计算以及 (g_v, h_v, R') 的计算, 其总的时间复杂度约为 $(0.75n + 19)\text{ct}$, 而验证者的计算开销主要是 (τ_x, t) 的验证以及 (g_v, h_v, R') 的计算, 其总的时间复杂度约为 $(0.5n + 12)\text{ct}$. 证明者和验证者运行内积向量承诺 $(\mathbb{G}, g_u, g_v, h_v, R', k; r, r')$ 所需的时间复杂度分别为 $(0.5n + 6.5 \log n - 15)\text{ct}$ 和 $(4.5 \log n - 7)\text{ct}$. 综上, 证明者产生证据的时间复杂度为 $(1.25n + 6.5 \log n + 4)\text{ct}$, 而验证者产生证据的时间复杂度为 $(0.5n + 4.5 \log n + 5)\text{ct}$, 证据的长度为 $(19 + 2 \log n)\text{cs}$.

接下来分析文献 [18] 中方案的计算复杂度和证据长度. 在运行内积向量承诺之前, 证明者花费的时间复杂度约为 $(2n + 3.5)\text{ct}$, 而验证者花费的时间复杂度约为 $(n + 6)\text{ct}$. 证明者和验证者运行内积向量承诺所需的时间复杂度分别为 $(n + 6.5 \log n - 8.5)\text{ct}$ 和 $(4.5 \log n - 2.5)\text{ct}$. 因此证明者总的时间复杂度约为 $(3n + 6.5 \log n - 5)\text{ct}$, 而验证者总的时间复杂度约为 $(n + 4.5 \log n + 3.5)\text{ct}$, 证据的长度为 $(9 + 2 \log n)\text{cs}$.

最后分析文献 [16] 和文献 [14] 方案的计算复杂度和证据长度, 并在表 2 中给出这四个方案的证据生成时间、证据验证时间以及证据长度. 值得一提的是, 文献 [16] 方案需要可信第三方的预计算, 且预计算的时间复杂度为 $(2^{n/m} + 0.5)\text{ct}$, 表中 ce 表示 G 上的双线性对的时间复杂度, 一般来说 $\text{ce} > 8.5\text{ct}$. 本文与文献 [18] 相比, 证据生成的时间和证据验证的时间均大大减少.

从表中可以看出, 在无中心的前提下, 本文的方案是非常有优势的. 值得一提的是, 工程实现一般选择 G 为满足离散对数困难的素数阶椭圆曲线群, 则文献 [14, 18] 以及本文所提出的方案具有很大的优化空间, 而文献 [16] 方案中证据的真实生成时间不会比本文方案的证据生成时间要少. 考虑到本文的方案在验证的时间复杂度上更有优势以及证据长度很小, 本文的方案更适合应用在区块链系统中.

表 2 范围证明方案的性能比较
Table 2 Performance comparison among range proof schemes

方案	证据生成时间	证据验证时间	证据长度	中心
文献 [16]	$(2.5m + 1)\text{ct} + (m)\text{ce}$	$(2.5m + 3)\text{ct} + (1.5m)\text{ce}$	$(3m + 2)\text{cs}$	有
文献 [14]	$(2.5n + 1)\text{ct}$	$(3n + 2)\text{ct}$	$(3n + 2)\text{cs}$	无
文献 [18]	$(3n + 6.5 \log n - 5)\text{ct}$	$(n + 4.5 \log n + 3.5)\text{ct}$	$(9 + 2 \log n)\text{cs}$	无
本文	$(1.25n + 6.5 \log n + 4)\text{ct}$	$(0.5n + 4.5 \log n + 5)\text{ct}$	$(19 + 2 \log n)\text{cs}$	无

5 结论

本文研究文献 [18] 的范围证明方案并结合该文献的零知识证明方案提出一种新的高效的范围证明方案, 新方案对金额进行两比特分割, 然后结合向量内积承诺构造相应的多项式承诺. 与文献 [18] 中的方案相比, 当范围区间为 $[0, 2^{64}]$ 时, 本文的方案将证明者的计算时间减少了近一半, 而将验证者的计算时间减少约 33%. 通过与文献 [14, 16, 18] 的方案相比, 本文的方案非常实用.

参考文献

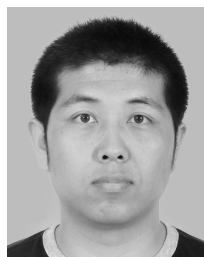
- [1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. 2008. <https://bitcoin.org/bitcoin.pdf>
- [2] NOETHER S. Ring signature confidential transactions for Monero[J]. IACR Cryptology ePrint Archive, 2015: 2015/1098. <https://eprint.iacr.org/2015/1098.pdf>
- [3] SUN S F, AU M H, LIU J K, et al. RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for Blockchain cryptocurrency Monero[C]. In: Computer Security—ESORICS 2017, Part II. Springer Cham, 2017: 456–474. [DOI: 10.1007/978-3-319-66399-9_25]
- [4] PETERSON P. Zcash—Transaction linkability[OL]. <https://z.cash/blog/transaction-linkability.html>, 2017.
- [5] LEE C. Litecoin[OL]. <https://litecoin.org>, 2011.
- [6] RIVEST R, SHAMIR A, TAUMAN Y. How to leak a secret[C]. In: Advances in Cryptology—ASIACRYPT 2001. Springer Berlin Heidelberg, 2001: 552–565. [DOI: 10.1007/3-540-45682-1_32]
- [7] BLUM M. Coin flipping by telephone[C]. In: Advances in Cryptology: A Report on CRYPTO '81, IEEE Workshop on Communications Security, Santa Barbara, CA, USA, August 24–26, 1981: 11–15.
- [8] GOLDBREICH O, OREN Y. Definitions and properties of zero-knowledge proof system[J]. Journal of Cryptology, 1994, 7(1): 1–32. [DOI: 10.1007/BF00195207]
- [9] PEDERSEN T. Non-interactive and information theoretic secure verifiable secret sharing[C]. In: Advances in Cryptology—CRYPTO '92. Springer Berlin Heidelberg, 1992: 129–140. [DOI: 10.1007/3-540-46766-1_9]
- [10] PARNO B, HOWELL J, GENTRY C, et al. Pinocchio: Nearly practical verifiable computation[C]. In: Proceedings of the 34th IEEE Symposium on Security and Privacy (SP). IEEE, 2013: 238–252. [DOI: 10.1109/SP.2013.47]
- [11] BEN-SASSON E, CHIESA A, GENKIN D, et al. SNARKs for C: Verifying program executions succinctly and in Zero Knowledge[C]. In: Advances in Cryptology—CRYPTO 2013, Part II. Springer Berlin Heidelberg, 2013: 90–108. [DOI: 10.1007/978-3-642-40084-1_6]
- [12] BEN-SASSON E, CHIESA A, TROMER E, et al. Succinct noninteractive arguments for a von Neumann architecture[J]. IACR Cryptology ePrint Archive, 2013: 2013/879. <https://eprint.iacr.org/2013/879.pdf>
- [13] SHAN J Y, GAO S. Research progress on theory of Blockchains[J]. Journal of Cryptologic Research, 2018, 5(5):

- 484–500. [DOI: 10.13868/j.cnki.jcr.000258]
 单进勇, 高胜. 区块链理论研究进展 [J]. 密码学报, 2018, 5(5): 484–500. [DOI: 10.13868/j.cnki.jcr.000258]
- [14] MAXWELL G. Confidential transactions[OL]. https://people.xiph.org/~greg/confidential_values.txt, 2016.
- [15] BONEH D, BOYEN X. Short signatures without random oracles[C]. In: Advances in Cryptology—EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 56–73. [DOI: 10.1007/978-3-540-24676-3_4]
- [16] CAMENISCH J, CHAABOUNI R, SHELAT A. Efficient protocols for set membership and range proofs[C]. In: Advances in Cryptology—ASIACRYPT 2008. Springer Berlin Heidelberg, 2008: 234–252. [DOI: 10.1007/978-3-540-89255-7_15]
- [17] MA S L, DENG Y, HE D B, et al. An efficient NIZK scheme for privacy-preserving transactions over account model Blockchain[J]. IACR Cryptology ePrint Archive, 2017: 2017/1239. <https://eprint.iacr.org/2017/1239.pdf>
- [18] BÜNZ B, BOOTLE J, BONEH D, et al. Bulletproofs: Efficient range proofs for confidential transactions[J]. IACR Cryptology ePrint Archive, 2017: 2017/1066. <https://eprint.iacr.org/2017/1066.pdf>
- [19] BOOTLE J, CERULLI A, CHAIDOS P, et al. Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting[C]. In: Advances in Cryptology—EUROCRYPT 2016, Part II. Springer Berlin Heidelberg, 2016: 327–357. [DOI: 10.1007/978-3-662-49896-5_12]
- [20] ZHANG F, HUANG N N, GAO S. Privacy data authentication schemes based on Borromean ring signature[J]. Journal of Cryptologic Research, 2018, 5(5): 529–537. [DOI: 10.13868/j.cnki.jcr.000262]
 张凡, 黄念念, 高胜. 基于 Borromean 环签名的隐私数据认证方案 [J]. 密码学报, 2018, 5(5): 529–537. [DOI: 10.13868/j.cnki.jcr.000262]
- [21] SHAFI G, SILVIO M, CHARLES R. The knowledge complexity of interactive proofs[J]. SIAM Journal on Computing, 1989, 18(1): 186–208. [DOI: 10.1137/0218012]
- [22] ODED G, SILVIO M, AVI W. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems[J]. Journal of the ACM, 1991, 38(3): 691–729. [DOI: 10.1145/116825.116852]
- [23] FEIGE U, FIAT A, SHAMIR A. Zero knowledge proofs of identify[J]. Journal of Cryptology, 1988, 1(2): 77–94. [DOI: 10.1007/BF02351717]
- [24] RIVEST R, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120–126. [DOI: 10.1145/359340.359342]
- [25] ALMUHAMRNADI S, SUI N T, MCLEOD D. Better privacy and security in E-commerce: Using elliptic curve based zero knowledge proofs[C]. In: Proceedings of IEEE International Conference on E-Commerce Technology. IEEE, 2004: 299–302. [DOI: 10.1109/ICECT.2004.1319747]
- [26] BOOTLE J, GROTH J. Efficient batch zero-knowledge arguments for low degree polynomials[C]. In: Public Key Cryptography—PKC 2018, Part II. Springer Cham, 2018: 561–588. [DOI: 10.1007/978-3-319-76581-5_19]
- [27] WAHBY R S, TZIALLA I, SHELAT A, et al. Doubly-efficient zkSNARKs without trusted setup[C]. In: Proceedings of 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018: 2375–1207. [DOI: 10.1109/SP.2018.00060]
- [28] WANG H G, CHEN K F, QIN B D, et al. LR-RRA-CCA secure functional encryption for randomized functionalities from trapdoor HPS and LAF[J]. SCIENCE CHINA Information Sciences, 2018, 61(5): 291–305. [DOI: 10.1007/s11432-017-9120-4]
- [29] WANG H G, CHEN K F, LIU J K, et al. Access control encryption with efficient verifiable sanitized decryption[J]. Information Sciences, 2018, 465: 72–85. [DOI: 10.1016/j.ins.2018.06.068]

作者信息



张凡 (1989–), 湖北孝感人, 博士, 工程师. 主要研究领域为区块链理论与技术.
 tzhangfan4@163.com



高胜 (1982–), 山西朔州人, 博士, 高级工程师. 主要研究领域为密码理论与应用.
 gs14011@163.com



曾志强(1972-), 内蒙古商都人, 硕士, 正高级工程师. 主要研究领域为网络与信息系统安全.
martinzeng2019@163.com



刘喆(1974-), 辽宁辽阳人, 硕士, 高级工程师. 主要研究领域为信息安全.
stayhere1974@163.com

中国密码学会 2020 年会征文通知

中国密码学会 2020 年会 (ChinaCrypt2020) 拟于 2020 年 10 月在贵州省贵阳市举办. 本次年会由中国密码学会主办、贵州大学和贵州省公共大数据重点实验室联合承办, 旨在汇聚国内外密码领域专家、学者、业界精英以及在校学生, 共同探讨密码学的最新研究成果、学术动态及发展趋势, 促进国内密码领域产学研用深度融合, 推动我国密码理论、技术与应用共同进步.

会议现面向全国从事密码学和信息安全领域的专家学者、科研工作者、工程技术人员以及在校研究生公开征稿.

一、征文内容

年会征文涵盖密码学理论和应用的各个分支. 征文范围包括但不限于: 对称密码、公钥密码、数字签名、杂凑函数、安全协议、密钥管理、后量子密码算法、量子密码学、混沌密码与混沌保密通信技术、生物特征密码技术、侧信道分析与泄露容忍密码算法、密码芯片、密码软件、大数据密码技术、区块链技术与应用、云计算安全、物联网与智能终端安全以及工控安全等. 会议将编辑年会论文集作为会议交流资料(不正式出版, 允许再投稿), 投稿论文可以是已向重要学术刊物或国际会议投稿或新近发表的高水平研究成果.

二、重要日期

论文投稿截止日期: 2020 年 9 月 15 日

论文录用通知日期: 2020 年 10 月 8 日

三、投稿要求

1. Email 发送电子稿, 联系和投稿邮箱为: cacr2020@cacrnnet.org.cn.
2. 来稿内容应是作者本人的科研成果, 数据真实、可靠, 具有较高的学术价值或应用价值.
3. 论文用 word 格式排版, 论文长度不做限制. 另附作者信息, 包括论文标题、作者、单位、Email 地址、通信地址、电话等.
4. 论文编排顺序如下: ① 标题; ② 作者; ③ 单位; ④ 中文摘要、关键词; ⑤ 英文摘要、关键词; ⑥ 正文; ⑦ 参考文献.

四、联系方式

稿件联系人: 丁红发 18786751281

投稿邮箱: cacr2020@cacrnnet.org.cn

会议网址: <http://cacr2020.cacrnnet.org.cn/fair/4>

中国密码学会

2020 年 4 月 3 日