Bulletproofs 论文解读

Author: Zelig(Twitter: @zelig_eth)

1. 预备知识

本节先介绍一些符号定义，然后介绍用到的背景知识，包括机密交易、范围证明等基础知识。

1.1. 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

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 $\boldsymbol{g}^{\boldsymbol{a}} = \prod_{j=1}^{n} g_j^{a_j}$, $\boldsymbol{g}^{x} = (g_1^x, g_2^x, \cdots, g_n^x)$, 这里 $\boldsymbol{g} = (g_1, g_2, \cdots, g_n) \in \mathbb{G}^n$, $\boldsymbol{a} = (a_1, a_2, \cdots, a_n) \in \mathbb{Z}_q^n$. 规定两个向量多项式 $\boldsymbol{a}(X), \boldsymbol{b}(X) \in \mathbb{Z}_q^n[X]$ 的乘积运算 $c(X) = \boldsymbol{a}(X) \cdot \boldsymbol{b}(X)$ 为多项式乘法并且系数之间的乘法定义为内积, 此时 $c(X) \in \mathbb{Z}_q[X]$.

1.2. 背景知识

基于区块链的加密货币可以通过维护一个全球分布式且同步的账本（区块链）来实现点对点电子价值转移。任何独立的观察者都可以验证区块链的当前状态以及账本上所有交易的有效性。在比特币中，这种创新性的行为要求交易的所有细节都是公开的，即发送者，接收者以及转移的金额信息都是透明的。总的来说，我们将支付的隐私权分为两个属性：

（1）匿名性：隐藏一笔交易中的发送者和接收者的身份；

（2）保密性：隐藏转账金额；

虽然比特币通过比特币的地址提供了一些弱的匿名性（之所以说弱匿名性是因为如果建立了公共地址和现实生活用户之间的关联性，其他用户就能够确切地知道他们正在与谁交易），但是它缺乏保密性。这对比特币在现实世界中的应用是一个严重的限制。比如说，如果一个员工接受公司使用比特币支付他们的工资，那么他就要面临一个问题：他的工资会公布到比特币的公共区块链上，这显然泄露了员工的隐私。

因此，比特币和其它加密货币，以及各类区块链项目发展的一大限制就是如何保证交易金额的机密性。

1.2.1. 机密交易

为了保证交易的保密性，Maxwell 在 2016 年提出了“机密交易”（Confidential Transactions）[1]的概念，即交易发起者不需要公布具体的交易金额，只需要对交易金额做出承诺并给出相应的证据证明该金额位于某个范围之内。注意，比特币和其他类似的加密货币使用的是基于交易输出的系统，即当前这笔交易其中的一个输入使用的是之前某笔交易的未使用过的一个输出，并且需要附加当前交易输入地址对应的数字签名。这种交易模式称为 UTXO（Unspent Transaction Outputs）模式。因此，这种模式的交易需要验证当前交易的每一个输入都是之前未使用过的一个输出，同时还要保证一笔交易的输入的和要大于输出的和。机密交易的思想就是用承诺算法将交易金额（UTXO 形式交易中的各个输入和输出）；同时为了支持公开可验证性，机密交易通过零知识证明来证明交易的输入总和大于输出总和，并且所有的输出都是正的。

Maxwell 在论文中使用 Pedersen 承诺方案[2]来隐藏交易金额，该方案将明文所表示的 UTXO

数值替换为加密承诺，同时，某个用户（私钥）与加密承诺绑定，表示用户持有加密承诺内包含的余额，但是该承诺不会显示余额的具体数值。接下来详细介绍一下 Pedersen 承诺。

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

定义 1 (Pedersen 承诺) $\mathrm{Com_{ck}}(a;r):=g^r h^a$ 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 $\mathrm{ck}=(\mathbb{G},q,g,h_1,\cdots,h_n)$, 这里 g 是 $\mathbb{G}$ 的生成元, $(h_1,\cdots,h_n)\in\mathbb{G}^n$, 这些点的离散对数均未知. 给定消息 $(m_1,\cdots,m_n)\in\mathbb{Z}_q^n$, 则对应的 Pedersen 承诺为

$$c=\mathrm{Com_{ck}}(m_1,\cdots,m_n;r)=g^r\prod_{i=1}^{n}h_i^{m_i}$$

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.

同时，Pedersen 承诺具有非常好的同态加密性(Homomorphic Encryption)，这个性质保证了 UTXO 交易中多个输入和输出的总和均是 Pedersen 承诺，即交易金额可隐藏。

1.2.2. 范围证明

使用了上面提到的 Pedersen 承诺解决了比特币隐私之后，还需要面临一个问题就是如果用户能够构造了一个对负值的承诺，比如说创建对-20BTC 输出的承诺，那么其他剩下输出的比特币的总额就会超出输入的总额。事实上这个漏洞之前在比特币的发展过程中也被黑客利用过，构造负值的输出无异于开动印钞机增发货币。

为了解决上面提到的问题，机密交易中引入了范围证明(Range Proof)[3]的技术来解决验证正负的问题。范围证明可以证明经过承诺或者加密等隐藏处理之后的某个秘密数的取值是位于某一个特定的区间之内的。

尽管范围证明方案作为机密交易的一个组成部分是非常有必要的，但是当前的范围证明方案面临两个主要问题：

(1) 需要可信第三方；

(2) 时间和空间上的巨大性能开销；

Maxwell 等人利用了 Borromean 环签名[4]给出了一个具体的范围证明的实现方案，尽管该方案不需要可信第三方的参与，但是这个方案依旧面临着性能开销问题：证据的生成和验证阶段的时间复杂度均与金额的比特数线性相关，并且证据的长度比较庞大。时间上，传统的 UTXO 交易的验证时间不会超过 100 微妙，但是引入了范围证明的机密交易的验证时间会变为几个毫秒；而空间上，在 Maxwell 等人的论文实现中，一笔仅带有两个输出以及 32 位精度的机密交易，其数据大小是 5.4KB，其中 5KB 是用来做范围证明的，即使经过优化之后，用来做范围证明的数据依旧占据了 3.8KB 的数据空间。因此，该方案在实际应用中非常受限。

Jan Camenisch 等人于 2008 年提出一种交互式的范围证明方案[5]，该方案是基于 Boneh-Boyen 签名[6]，该方案后来被 Shunli Ma 等人[7]借鉴用来保护交易金额的隐私性, 该方案需要可信第三方的参与并采用了双线性对，优势在于证据长度很短, 但是验证时间比较长。2017 年, Benedikt Bun 等人[8]提出新的范围证明方案，即本报告所研究的 Bulletproofs 方案, 该方案借鉴 Jonathan Bootle[9]等人提出的基于多项式承诺的零知识证明方案, 并采用了向量内积承诺方案从而将证据长度减为对数级别。该方案突破了以往范围证明方案的限制，不仅不需要可信第三方的参与, 减少证据验证的时间复杂度, 并且将证据长度大大降低, 这些特性也让该方案能很好地应

用在区块链系统中。

2. Bulletproofs 原理

接下来将对 Bulletproofs 技术的原理进行详细分析。首先介绍一下向量内积承诺。

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

下面介绍一下 Bootle 等人提出的向量内积承诺，Bulletproofs 方案构造在该方案的基础上并进行了相应的改进。

不妨将该方案记作 $(G,\boldsymbol{g},\boldsymbol{h},A,B,c,n;\boldsymbol{a},\boldsymbol{b})$，这里 $\boldsymbol{g},\boldsymbol{h}$ 中每个元素的离散对数都是未知的并且 n 为 2 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

$$\boldsymbol{g}=(\boldsymbol{g}_1,\boldsymbol{g}_2),\quad \boldsymbol{h}=(\boldsymbol{h}_1,\boldsymbol{h}_2),\quad \boldsymbol{a}=(\boldsymbol{a}_1,\boldsymbol{a}_2),\quad \boldsymbol{b}=(\boldsymbol{b}_1,\boldsymbol{b}_2)$$

这里 $\boldsymbol{g}_1,\boldsymbol{g}_2,\boldsymbol{h}_1,\boldsymbol{h}_2\in\mathbb{G}^{n/2},\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{b}_1,\boldsymbol{b}_2\in\mathbb{Z}_q^{n/2}$, 则

$$A=\boldsymbol{g}_1^{\boldsymbol{a}_1}\boldsymbol{g}_2^{\boldsymbol{a}_2},\quad B=\boldsymbol{h}_1^{\boldsymbol{b}_1}\boldsymbol{h}_2^{\boldsymbol{b}_2},\quad c=\boldsymbol{a}\cdot\boldsymbol{b}=\boldsymbol{a}_1\cdot\boldsymbol{b}_1+\boldsymbol{a}_2\cdot\boldsymbol{b}_2$$

然后令 $\boldsymbol{a}'(X)=\boldsymbol{a}_1X+\boldsymbol{a}_2X^2,\boldsymbol{b}'(X)=\boldsymbol{b}_1X^{-1}+\boldsymbol{b}_2X^{-2}$, 于是 $\boldsymbol{a}'(X)\cdot\boldsymbol{b}'(X)$ 的常数项等于 c. 设随机数 $x\in\mathbb{Z}_q^*$, 令 $\boldsymbol{a}'=\boldsymbol{a}'(x),\boldsymbol{b}'=\boldsymbol{b}'(x)$ 以及 $\boldsymbol{g}'=\boldsymbol{g}_1^{x^{-1}}\circ\boldsymbol{g}_2^{x^{-2}},\boldsymbol{h}'=\boldsymbol{h}_1^{x}\circ\boldsymbol{h}_2^{x^2}$, 则

$$\begin{aligned}
&(\boldsymbol{g}')^{\boldsymbol{a}'}=A_{-1}^{x^{-1}}A_0A_1^x,\quad \text{这里}A_{-1}=\boldsymbol{g}_2^{\boldsymbol{a}_1},A_0=\boldsymbol{g}_1^{\boldsymbol{a}_1}\boldsymbol{g}_2^{\boldsymbol{a}_2},A_1=\boldsymbol{g}_1^{\boldsymbol{a}_2},\\
&(\boldsymbol{h}')^{\boldsymbol{b}'}=B_{-1}^{x^{-1}}B_0B_1^x,\quad \text{这里}B_{-1}=\boldsymbol{h}_1^{\boldsymbol{b}_2},B_0=\boldsymbol{h}_1^{\boldsymbol{b}_1}\boldsymbol{h}_2^{\boldsymbol{b}_2},B_1=\boldsymbol{h}_2^{\boldsymbol{b}_1},\\
&c'=\boldsymbol{a}'\cdot\boldsymbol{b}'=c_{-1}x^{-1}+c_0+c_1x,\quad \text{这里}c_{-1}=\boldsymbol{a}_1\cdot\boldsymbol{b}_2,c_0=\boldsymbol{a}_1\cdot\boldsymbol{b}_2+\boldsymbol{a}_1\cdot\boldsymbol{b}_2,c_1=\boldsymbol{a}_2\cdot\boldsymbol{b}_1
\end{aligned}$$

如果令 $A'=(\boldsymbol{g}')^{\boldsymbol{a}'},B'=(\boldsymbol{h}')^{\boldsymbol{b}'}$, 则原向量内积承诺转化为对新向量 $\boldsymbol{a}'$ 和 $\boldsymbol{b}'$ 的内积承诺. 注意到验证者需要计算 $\boldsymbol{g}',\boldsymbol{h}',A',B'$ 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 $(\mathbb{G},\boldsymbol{g},\boldsymbol{h},A,B,c,n;\boldsymbol{a},\boldsymbol{b})$ 的具体过程, 这里只有 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 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: $\boldsymbol{g}, \boldsymbol{h} \in \mathbb{G}^n, A, B \in \mathbb{G}, c \in \mathbb{Z}_q^*$, 并且假设 n 为二的幂次方.

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

协议过程: (1) 当 $(n > 1)$ 时, 执行递归约减步骤:

- P→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←V: 发送随机数 $x \in \mathbb{Z}_q^*$;
- P→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

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

这里

$$\begin{aligned} \boldsymbol{g}' &= \boldsymbol{g}_1^{x^{-1}} \circ \boldsymbol{g}_2^{x^{-2}}, A' = A_{-1}^{x^{-1}} A_0 A_1^x \\ \boldsymbol{h}' &= \boldsymbol{h}_1^x \circ \boldsymbol{h}_2^{x^2}, \quad B' = B_{-1}^{x^{-1}} B_0 B_1^x \\ \boldsymbol{c}' &= c_{-1} x^{-1} + c_0 + c_1 x \end{aligned}$$

此外, P 还需更新自己的秘密输入, 即 $\boldsymbol{a}' = \boldsymbol{a}_1 x + \boldsymbol{a}_2 x^2$ 和 $\boldsymbol{b}' = \boldsymbol{b}_1 x^{-1} + \boldsymbol{b}_2 x^{-2}$.

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→V: P 直接发送 (a, b);
- P←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，所需的通信带宽比较大，为了降低通信复杂度，Bulletproofs 论文中提出了一种优化后的向量内积承诺。

该方案考虑 $P = \boldsymbol{g}^{\boldsymbol{a}} \boldsymbol{h}^{\boldsymbol{b}} g_t^{\ c}$，这里 $c = \boldsymbol{a}, \boldsymbol{b}$，$g_t$ 的离散对数未知。此时在递归约减的步骤中 A_i, B_i 以及 c_i 可以合并发送，不妨将该承诺方案记做 $(G, g_t, \boldsymbol{g}, \boldsymbol{h}, P, n; \boldsymbol{a}, \boldsymbol{b})$,下面是其具体过程。

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

秘密输入: 证明者拥有 $\boldsymbol{a} = (\boldsymbol{a}_1, \boldsymbol{a}_2), \boldsymbol{b} = (\boldsymbol{b}_1, \boldsymbol{b}_2)$ 并满足 $P = \boldsymbol{g}_1^{\boldsymbol{a}_1} \boldsymbol{g}_2^{\boldsymbol{a}_2} \boldsymbol{h}_1^{\boldsymbol{b}_1} \boldsymbol{h}_2^{\boldsymbol{b}_2} g_t^c$, 这里

$$\boldsymbol{g}=(\boldsymbol{g}_1,\boldsymbol{g}_2),\quad \boldsymbol{h}=(\boldsymbol{h}_1,\boldsymbol{h}_2),\quad c=\boldsymbol{a}_1\cdot\boldsymbol{b}_1+\boldsymbol{a}_2\cdot\boldsymbol{b}_2$$

协议过程: 如果 $n=1$, 则

- P→V: 直接发送 (a,b)
- P←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→V: 发送 (L,R), 这里 $L=\boldsymbol{g}_2^{\boldsymbol{a}_1}\boldsymbol{h}_1^{\boldsymbol{b}_2}g_t^{c_L}$, $c_L=\boldsymbol{a}_1\cdot\boldsymbol{b}_2\in\mathbb{Z}_q$, $R=\boldsymbol{g}_1^{\boldsymbol{a}_2}\boldsymbol{h}_2^{\boldsymbol{b}_1}g_t^{c_R}$, $c_R=\boldsymbol{a}_2\cdot\boldsymbol{b}_1\in\mathbb{Z}_q$.
- P←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

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

这里

$$\boldsymbol{g}'=\boldsymbol{g}_1^{x^{-1}}\circ\boldsymbol{g}_2^{x^{-2}},\quad \boldsymbol{h}'=\boldsymbol{h}_1^{x}\circ\boldsymbol{h}_2^{x^2},\quad P'=L^{x^{-1}}PR^{x}$$

而且证明者还需计算

$$\boldsymbol{a}'=\boldsymbol{a}_1x+\boldsymbol{a}_2x^2\in\mathbb{Z}_q^{n'},\quad \boldsymbol{b}'=\boldsymbol{b}_1x^{-1}+\boldsymbol{b}_2x^{-2}\in\mathbb{Z}_q^{n'}$$

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.

有了向量内积承诺方案的背景之后，接下来分几步介绍 Bulletproofs 如何进行范围证明。

(1) 陈述证明

首先，令 $v\in Z_p$，$V=h^{\gamma}g^{v}$，即 V 是 v 的 Pedersen 承诺，其中 γ 是随机数。整个证明系统想要说服验证者 $v\in[0,2^n-1]$，也就是说整个证明系统想要证明如下关系：

$$\left\{(g,h\in\mathbb{G},V,n\ ;\ v,\gamma\in\mathbb{Z}_p):V=h^{\gamma}g^{v}\wedge v\in[0,2^n-1]\right\}$$

其中 g,h,V,n 是公开的信息，然后 v,γ 是不能公开的信息。

假设 $\boldsymbol{a}_L=(a_1,a_2,\cdots,a_n)\in\{0,1\}^n$ 是 v 的各个比特位组成的向量, 我们可知 $<\boldsymbol{a}_L,\boldsymbol{2}^n>=v$，其中 $\boldsymbol{2}^n=(1,2,4,\cdots,2^{n-1})$。同时，我们必须保证 $\boldsymbol{a}_L$ 中每个元素的值只能为 0 或者 1，也就是要满足如下关系：

$$\begin{aligned}&<\boldsymbol{a}_L,\boldsymbol{2}^n>=v\\&\boldsymbol{a}_R=\boldsymbol{a}_L-\boldsymbol{1}^n\\&\boldsymbol{a}_R\circ\boldsymbol{a}_L=\boldsymbol{0}^n\end{aligned}\tag{1}$$

此时范围证明的基本信息可以表示为：

公开信息：$g,h\in G,\boldsymbol{g},\boldsymbol{h}\in G^n,A,V\in G,n$

私密信息：$v,\gamma,\alpha\in Z_p,\boldsymbol{a}_R,\boldsymbol{a}_L$

关系：

$$
\begin{aligned}
&V = h^{\gamma} g^{v} \\
&A = h^{\alpha} \boldsymbol{g}^{\boldsymbol{\alpha}_L} \boldsymbol{h}^{\boldsymbol{\alpha}_R} \\
&< \boldsymbol{\alpha}_L, \boldsymbol{2}^n >= v \\
&\boldsymbol{\alpha}_R = \boldsymbol{\alpha}_L - \boldsymbol{1}^n \\
&\boldsymbol{\alpha}_R \circ \boldsymbol{\alpha}_L = \boldsymbol{0}^n
\end{aligned} \tag{2}
$$

接下来我们希望将关系(2)中的最后三个等式中所包含的 2n+1 个约束压缩为一个向量内积约束的形式。从而我们可以使用上面提到的向量内积承诺的协议来证明整个向量内积的关系是成立的。

(2) 压缩为一个向量内积约束

首先我们明确这样一件事情，如果要证明一个向量 $\boldsymbol{b} \in Z_p^n$ 满足 $\boldsymbol{b} = \boldsymbol{0}^n$，只要验证者发送一个随机数 $y \in Z_p$，然后证明者证明 $< \boldsymbol{b}, \boldsymbol{y}^n >= 0$。如果 $\boldsymbol{b} \neq \boldsymbol{0}^n$，那么前式成立的概率是可以忽略的。所以，如果 $< \boldsymbol{b}, \boldsymbol{y}^n >= 0$，那么就可以让验证者相信 $\boldsymbol{b} = \boldsymbol{0}^n$。

基于上述观察，验证者发送随机数 $y \in Z_p$，证明者需要证明的关系可转化为下面的关系：

$$
\begin{aligned}
&< \boldsymbol{\alpha}_L, \boldsymbol{2}^n >= v \\
&< \boldsymbol{\alpha}_L, \boldsymbol{\alpha}_R \circ \boldsymbol{y}^n >= 0 \\
&< \boldsymbol{\alpha}_L - \boldsymbol{\alpha}_R - \boldsymbol{1}^n, \boldsymbol{y}^n >= 0
\end{aligned} \tag{3}
$$

进一步，验证者可以发送随机数 $z \in Z_p$，然后将关系(3)转化为如下关系：

$$
z^2 \cdot < \boldsymbol{\alpha}_L, \boldsymbol{2}^n > + z \cdot < \boldsymbol{\alpha}_L - \boldsymbol{\alpha}_R - \boldsymbol{1}^n, \boldsymbol{y}^n > + < \boldsymbol{\alpha}_L, \boldsymbol{\alpha}_R \circ \boldsymbol{y}^n >= z^2 \cdot v \tag{4}
$$

(3)合并内积

我们需要将关系(4)进行进一步的合并，转化成为一个内积的形式，在转化之后的内积中，$\boldsymbol{\alpha}_L$ 只出现在左边，$\boldsymbol{\alpha}_R$ 只出现在右边，并且将包含秘密信息的那些项统一合并起来记为 δ。

具体来说，将关系(4)展开之后，重新排列，然后两边同时加上 $< -z \cdot \boldsymbol{1}^n, z^2 \cdot \boldsymbol{2}^n + z \cdot \boldsymbol{y}^n >$ 之后接着进行化简，同时注意到有 $\boldsymbol{y}^n = \boldsymbol{y}^n \circ \boldsymbol{1}^n$，$< \boldsymbol{\alpha}_R, \boldsymbol{y}^n >=< \boldsymbol{1}^n, \boldsymbol{\alpha}_R \circ \boldsymbol{y}^n >$，则关系(4)可以重新写为：

$$
< \boldsymbol{\alpha}_L - z \cdot \boldsymbol{1}^n, \boldsymbol{y}^n \circ (\boldsymbol{\alpha}_R + z \cdot \boldsymbol{1}^n) + z^2 \cdot \boldsymbol{2}^n >= z^2 \cdot v + \delta(y, z) \tag{5}
$$

其中，$\delta(y, z) = (z - z^2) < \boldsymbol{1}^n, \boldsymbol{y}^n > - z^3 < \boldsymbol{1}^n, \boldsymbol{2}^n >$，验证者很容易计算出该值。

至此，范围证明的基本信息如下：

公开信息：$g, h \in G, \boldsymbol{g}, \boldsymbol{h} \in G^n, A, V \in G, n$

验证者发送的随机挑战： $y,z \in Z_p^*$

私密信息： $v,\gamma,\alpha \in Z_p, \boldsymbol{a}_R, \boldsymbol{a}_L$

关系：

$$V = h^{\gamma} g^{v}$$

$$A = h^{\alpha} \boldsymbol{g}^{\boldsymbol{a}_L} \boldsymbol{h}^{\boldsymbol{a}_R} \tag{6}$$

$$< \boldsymbol{a}_L - z \cdot \boldsymbol{1}^n, \boldsymbol{y}^n \circ (\boldsymbol{a}_R + z \cdot \boldsymbol{1}^n) + z^2 \cdot \boldsymbol{2}^n >= z^2 \cdot v + \delta(y,z)$$

其中 $\delta(y,z) = (z - z^2) < \boldsymbol{1}^n, \boldsymbol{y}^n > - z^3 < \boldsymbol{1}^n, \boldsymbol{2}^n >$

(4) 内积盲化

如果证明者直接将关系(6)中的内积中的两个向量发送给验证者，验证者可以通过直接验证 $Com(< \boldsymbol{a}_L - z \cdot \boldsymbol{1}^n, \boldsymbol{y}^n \circ (\boldsymbol{a}_R + z \cdot \boldsymbol{1}^n) + z^2 \cdot \boldsymbol{2}^n > - \delta(y,z)) = Com(v)^{z^2}$ 是否成立来判断关系(6)是否成立。但是，关系(6)中的内积的左边的向量包含了 $\boldsymbol{a}_L$，直接发送该向量会泄露信息。为了解决该问题，方案中接着引入了盲化因子 $\boldsymbol{s}_L, \boldsymbol{s}_R \in Z_p^n$ 来隐藏要发送的向量。

在介绍证明者使用盲化因子之前，我们首先梳理一下证明者和验证者的交互过程。

$\mathcal{P}_{\mathsf{IP}}$ on input v, γ computes:

$\mathbf{a}_L \in \{0,1\}^n$ s.t. $\langle \mathbf{a}_L, \mathbf{2}^n \rangle = v$

$\mathbf{a}_R = \mathbf{a}_L - \mathbf{1}^n \in \mathbb{Z}_p^n$

$\alpha \xleftarrow{\$} \mathbb{Z}_p$

$A = h^{\alpha} \mathbf{g}^{\mathbf{a}_L} \mathbf{h}^{\mathbf{a}_R} \in \mathbb{G}$ // *commitment to* $\mathbf{a}_L$ *and* $\mathbf{a}_R$

$\mathbf{s}_L, \mathbf{s}_R \xleftarrow{\$} \mathbb{Z}_p^n$ // *choose blinding vectors* $\mathbf{s}_L, \mathbf{s}_R$

$\rho \xleftarrow{\$} \mathbb{Z}_p$

$S = h^{\rho} \mathbf{g}^{\mathbf{s}_L} \mathbf{h}^{\mathbf{s}_R} \in \mathbb{G}$ // *commitment to* $\mathbf{s}_L$ *and* $\mathbf{s}_R$

$\mathcal{P} \rightarrow \mathcal{V} : A, S$

$\mathcal{V} : y, z \xleftarrow{\$} \mathbb{Z}_p^{\star}$ // *challenge points*

$\mathcal{V} \rightarrow \mathcal{P} : y, z$

图 1 交互过程 1

在前面交互的基础上，证明者使用 $\boldsymbol{s}_L, \boldsymbol{s}_R$ 来构造以下多项式：

$$\begin{aligned} l(X) &= (\boldsymbol{a}_L + \boldsymbol{s}_L \cdot X) - z \cdot \boldsymbol{1}^n \in Z_p^n[X] \\ r(X) &= \boldsymbol{y}^n \circ ((\boldsymbol{a}_R + \boldsymbol{s}_R \cdot X) + z \cdot \boldsymbol{1}^n) + z^2 \cdot \boldsymbol{2}^n \in Z_p^n[X] \\ t(X) &= < l(X), r(X) >= t_0 + t_1 \cdot X + t_2 \cdot X^2 \in Z_p[X] \end{aligned} \tag{7}$$

可以看到 $l(X)$ 和 $r(X)$ 相当于使用 $\boldsymbol{a}_L + \boldsymbol{s}_L \cdot X$ 和 $\boldsymbol{a}_R + \boldsymbol{s}_R \cdot X$ 来隐藏 $\boldsymbol{a}_L, \boldsymbol{a}_R$，我们可以发现

$t_0 = < \boldsymbol{\alpha}_L - z \cdot \boldsymbol{1}^n, \boldsymbol{y}^n \circ (\boldsymbol{\alpha}_R + z \cdot \boldsymbol{1}^n) + z^2 \cdot \boldsymbol{2}^n >$，而盲化因子 $\boldsymbol{s}_L, \boldsymbol{s}_R$ 保证了证明者在发送 $l(X)$ 和 $r(X)$ 的时候不会泄露任何关于 $\boldsymbol{\alpha}_L, \boldsymbol{\alpha}_R$ 的信息。

所以我们接下来需要证明者证明如下关系：

$$t_0 = z^2 \cdot v + \delta(y, z) \tag{8}$$

关系(8)成立的前提是 $t(X)$ 是正确的多项式，即我们不光要证明关系(8)，同时需要证明 $t(X)$ 是正确的多项式，而证明 $t(X)$ 是正确的多项式等价于证明 $l(X), r(X)$ 均是正确的，并且 $t(X) = < l(X), r(X) >$。即证明关系(8)等价于证明以下两点：

- $t_0 = z^2 \cdot v + \delta(y, z)$ (8)
- $l(X), r(X)$ 均是正确的，并且 $t(X) = < l(X), r(X) >$ (9)

（5）证明正确性

要证明关系(8)，证明者可以首先制作一个关于 $t(X)$ 系数的承诺，然后通过准确回答验证者给出的任意挑战值来向验证者证明这些承诺是对 $t(X)$ 系数的正确承诺。注意，证明者已经用承诺 V 承诺了 v（本质上是承诺了 t_0），因此证明者需要再计算关于 t_1 和 t_2 的承诺 T_1 和 T_2，并且把这些承诺发送给验证者。

至此，范围证明的基本信息如下：

公开信息：$g, h \in G, \boldsymbol{g}, \boldsymbol{h} \in G^n, A, V, S \in G, \boldsymbol{l}, \boldsymbol{r} \in Z_p^n, \hat{t} \in Z_p, T_1, T_2 \in G, n$

验证者发送的随机挑战：$y, z, x \in Z_p^*$

私密信息：$v, \gamma, \alpha \in Z_p, \boldsymbol{\alpha}_R, \boldsymbol{\alpha}_L \in Z_p^n, \rho \in Zs_p, \boldsymbol{s}_L, \boldsymbol{s}_R \in Z_p^n, t_1, t_2 \in Z_p, \tau_1, \tau_2 \in Z_p$

关系：

$$V = h^{\gamma} g^{v}$$

$$A = h^{\alpha} \boldsymbol{g}^{\boldsymbol{\alpha}_L} \boldsymbol{h}^{\boldsymbol{\alpha}_R}$$

$$S = h^{\rho} \boldsymbol{g}^{\boldsymbol{s}_L} \boldsymbol{h}^{\boldsymbol{s}_R}$$

$$T_1 = h^{\tau_1} g^{t_1}$$

$$T_2 = h^{\tau_2} g^{t_2}$$

$$\hat{t} = < \boldsymbol{l}, \boldsymbol{r} >$$

$$\boldsymbol{l} = l(x) = (\boldsymbol{a}_L + \boldsymbol{s}_L \cdot x) - z \cdot \boldsymbol{1}^n$$

$$\boldsymbol{r} = r(x) = \boldsymbol{y}^n \circ ((\boldsymbol{a}_R + \boldsymbol{s}_R \cdot x) + z \cdot \boldsymbol{1}^n) + z^2 \cdot \boldsymbol{2}^n$$

接下来，证明者和验证者在图一交互过程的基础上进行如下交互。

$\mathcal{P}_{\mathsf{IP}}$ computes:

$\tau_1, \tau_2 \xleftarrow{\$} \mathbb{Z}_p$

$T_i = g^{t_i} h^{\tau_i} \in \mathbb{G}, \quad i = \{1, 2\}$ // *commit to* t_1, t_2

$\mathcal{P} \to \mathcal{V} : T_1, T_2$

$\mathcal{V} : x \xleftarrow{\$} \mathbb{Z}_p^\star$

$\mathcal{V} \to \mathcal{P} : x$ // *a random challenge*

$\mathcal{P}_{\mathsf{IP}}$ computes:

$\mathbf{l} = l(x) = \mathbf{a}_L - z \cdot \mathbf{1}^n + \mathbf{s}_L \cdot x \in \mathbb{Z}_p^n$

$\mathbf{r} = r(x) = \mathbf{y}^n \circ (\mathbf{a}_R + z \cdot \mathbf{1}^n + \mathbf{s}_R \cdot x) + z^2 \cdot \mathbf{2}^n \in \mathbb{Z}_p^n$

$\hat{t} = \langle \mathbf{l}, \mathbf{r} \rangle \in \mathbb{Z}_p$ // $\hat{t} = t(x)$

$\tau_x = \tau_2 \cdot x^2 + \tau_1 \cdot x + z^2 \cdot \gamma \in \mathbb{Z}_p$ // *blinding value for* $\hat{t}$

$\mu = \alpha + \rho \cdot x \in \mathbb{Z}_p$ // α, ρ *blind* A, S

$\mathcal{P} \to \mathcal{V} : \tau_x, \mu, \hat{t}, \mathbf{l}, \mathbf{r}$

图 2 交互过程 2

注意有 $A = Com_{ck}(\boldsymbol{a}_L, \boldsymbol{a}_R; \alpha) = h^\alpha \boldsymbol{g}^{\boldsymbol{a}_L} \boldsymbol{h}^{\boldsymbol{a}_R} = Com_{ck'}(\boldsymbol{a}_L, \boldsymbol{a}_R \circ \boldsymbol{y}^n; \alpha) = h^\alpha \boldsymbol{g}^{\boldsymbol{a}_L} \boldsymbol{h}'^{(\boldsymbol{a}_R \circ \boldsymbol{y}^n)}$，其中 $\boldsymbol{h}' = \boldsymbol{h}^{\boldsymbol{y}^{-n}} = (h_1, h_2^{y^{-1}}, h_3^{y^{-2}}, \cdots, h_n^{y^{-n+1}})$，同理对 S 也可以做同样的推导。接下来验证者可以利用承诺的同态性做如下校验。

$h'_i = h_i^{(y^{-i+1})} \in \mathbb{G}, \quad \forall i \in [1, n]$ // $\mathbf{h}' = \left(h_1, h_2^{(y^{-1})}, h_3^{(y^{-2})}, \ldots, h_n^{(y^{-n+1})}\right)$

$g^{\hat{t}} h^{\tau_x} \stackrel{?}{=} V^{z^2} \cdot g^{\delta(y,z)} \cdot T_1^x \cdot T_2^{x^2}$ // *check that* $\hat{t} = t(x) = t_0 + t_1 x + t_2 x^2$

$P = A \cdot S^x \cdot \mathbf{g}^{-z} \cdot (\mathbf{h}')^{z \cdot \mathbf{y}^n + z^2 \cdot \mathbf{2}^n} \in \mathbb{G}$ // *compute a commitment to* $l(x), r(x)$

$P \stackrel{?}{=} h^\mu \cdot \mathbf{g}^{\mathbf{l}} \cdot (\mathbf{h}')^{\mathbf{r}}$ // *check that* $\mathbf{l}, \mathbf{r}$ *are correct*

$\hat{t} \stackrel{?}{=} \langle \mathbf{l}, \mathbf{r} \rangle \in \mathbb{Z}_p$ // *check that* $\hat{t}$ *is correct*

图 3 验证者校验过程

通过验证者的校验过程我们可以看出实际上校验的第二个等式就证明了关系(8)，而最后两个等式就证明了(9)。

至此，我们已经可以通过上面提到的交互过程完成范围证明。

(6)优化

在图二的交互过程的最后我们可以看到证明者给验证者发送的是 $\boldsymbol{l}, \boldsymbol{r}$，我们可以利用之前提到的向量内积承诺来优化我们的交互过程。

我们在前面提到的第一种向量内积承诺方案其实就是一个证明如下关系的证明系统:

$$\{(\boldsymbol{g}, \boldsymbol{h} \in G^n, P \in G, c \in Z_p; \boldsymbol{a}, \boldsymbol{b} \in Z_p^n) : P = \boldsymbol{g}^{\boldsymbol{a}} \boldsymbol{h}^{\boldsymbol{b}}, c = < \boldsymbol{a}, \boldsymbol{b} >\}$$

其公开输入为$(\boldsymbol{g},\boldsymbol{h},P,c)$，而证明者给发送者发送$\boldsymbol{l},\boldsymbol{r}$以及验证者校验的过程（图三中的最后两步），其实就是一个内积承诺方案的交互过程。

该过程可以视为证明如下关系的证明系统：

$$\{(\boldsymbol{g},\boldsymbol{h}^{'}\in G^{n},Ph^{-\mu}\in G,\hat{t}\in Z_{p};\boldsymbol{l},\boldsymbol{r}\in Z_{p}^{n}):Ph^{-\mu}=\boldsymbol{g}^{\boldsymbol{l}}\boldsymbol{h}^{'\boldsymbol{r}},\hat{t}=<\boldsymbol{l},\boldsymbol{r}>\}$$

其公开输入变为$(\boldsymbol{g},\boldsymbol{h}^{'},Ph^{-\mu},\hat{t})$。同样，我们可以利用前面提到的第二种向量内积承诺方案的优化方式优化这个证明过程的通信复杂度，整个向量内积协议只需要传输$2\lceil\log_{2}(n)\rceil+2$个元素。

至此，阐述了一个交互式的高效的范围证明，最终整个范围证明的过程中，证明者总共发送了$2\lceil\log_{2}(n)\rceil+9$个元素。

3. 聚合多个范围证明

Dagher 等人在 2015 年的论文《Privacy-preserving proofs of solvency for bitcoin exchanges (full version)》[10] 中提出了 Provisions 协议，用于证明交易所可偿还能力。Provision 协议中要求为每个账号金额均提供范围证明。

前面我们提到了如何使用 Bulletproofs 对一个值 *v* 进行范围证明，当然我们可以对多个值逐个进行范围证明，但是显然这样是十分低效的，我们希望通过修改 Bulletproofs 的证明过程来达到高效地证明多个值位于一个范围之内。

首先，将要证明的关系表述如下 ：

$$\{(g,h\in G,\boldsymbol{V}\in G^{m};\boldsymbol{v},\gamma\in Z_{p}^{m}):V_{j}=h^{\gamma_{j}}g^{v_{j}},v_{j}\in[0,2^{n}-1]\quad\forall j\in[1,m]\}$$

我们将 *m* 个值（每个值具有 *n* 比特）直接拼接到一起，然后为这 *n*m* 个比特提供范围证明。总体上范围证明的过程与之前的类似，但是需要对一些地方做如下修改。

首先，在图一交互过程中，证明者需要计算的$\boldsymbol{a}_{L}$发生了变化，证明者需要计算$\boldsymbol{a}_{L}\in Z_{p}^{n\cdot m}$使得$<\boldsymbol{2}^{n},\boldsymbol{a}_{L[(j-1)\cdot n:j\cdot n-1]}>=v_{j}$对于所有的$j\in[1,m]$（注意，$\boldsymbol{a}_{L}$右下角的方括号代表从第几比特到第几比特，比如*j=1*，表示从第 0 比特到第 *n*-1 比特），即$\boldsymbol{a}_{L}$是将每一个v_{j}的比特形式串联起来。同样地，我们需要相应地调整$l(X)$和$r(X)$。

$$l(X)=(\mathbf{a}_{L}-z\cdot\mathbf{1}^{n\cdot m})+\mathbf{s}_{L}\cdot X\in\mathbb{Z}_{p}^{n\cdot m}[X]$$

$$r(X)=\mathbf{y}^{n\cdot m}\circ(\mathbf{a}_{R}+z\cdot\mathbf{1}^{n\cdot m}+\mathbf{s}_{R}\cdot X)+\sum_{j=1}^{m}z^{1+j}\cdot\left(\mathbf{0}^{(j-1)\cdot n}\,\|\,\mathbf{2}^{n}\,\|\,\mathbf{0}^{(m-j)\cdot n}\right)\in\mathbb{Z}_{p}^{n\cdot m}$$

在计算τ_{x}的过程中，我们需要做如下修改。

$$\tau_{x}=\tau_{1}\cdot x+\tau_{2}\cdot x^{2}+\textstyle\sum_{j=1}^{m}z^{1+j}\cdot\gamma_{j},$$

相应地，$\delta(y,z)$也需要按照如下形式进行计算。

$$\delta(y,z) = (z-z^2)\cdot\langle \mathbf{1}^{n\cdot m}, \mathbf{y}^{n\cdot m}\rangle - \sum_{j=1}^{m} z^{j+2}\cdot\langle \mathbf{1}^{n}, \mathbf{2}^{n}\rangle$$

在图三验证者的验证过程中，需要将第二个等式变为包含所有V_j承诺的形式。

$$g^{\tilde{t}} h^{\tau_x} \stackrel{?}{=} g^{\delta(y,z)}\cdot \mathbf{V}^{z^2\cdot\mathbf{z}^m}\cdot T_1^{x}\cdot T_2^{x^2}$$

同时修改 *P* 的计算过程。

$$P = AS^{x}\cdot \mathbf{g}^{-z}\cdot \mathbf{h}'^{z\cdot\mathbf{y}^{n\cdot m}} \prod_{j=1}^{m} \mathbf{h}'^{z^{j+1}\cdot\mathbf{2}^{n}}_{[(j-1)\cdot n : j\cdot n-1]}$$

通过以上过程我们可以发现，对 *m* 个值的范围证明，证明者需要发送$2\lceil \log_2(m\cdot n)\rceil + 9$个元素，相比于单个元素的范围证明，仅仅增加了$2\log_2 m$个元素。

接下来我们将 Bulletproofs 协议和 Andrew Poelstra 等人在《Confidential assets》[11]中提到的范围证明方案以及Σ-protocol 范围证明方案[12]进行对比。

m range proofs for range $[0, 2^n - 1]$

	# $\mathbb{G}$ elements	# $\mathbb{Z}_p$ elements
Σ Protocol [CD98]	mn	$3mn + 1$
Poelstra et al. [PBF+]	$0.63 \cdot mn$	$1.26 \cdot mn + 1$
Bulletproofs	$2(\log_2(n) + \log_2(m)) + 4$	5

图 4 几种不同的范围证明方案对比

在上图中，当 *m*=1 的时候代表对单个值进行范围证明，通过上图我们可以看出对，多个值的范围证明，Bulletproofs 优势十分明显，随着值的个数 *m* 的增加，Bulletproofs 方案中证明者发送的元素的个数增加了$2\log_2 m$，而其他方案都是成 *m* 倍增加。

4. 实现非交互式的范围证明

Fiat-Shamir 变换[13]可以将交互式的证明过程转换为非交互式，同样地，我们也可以对上面的协议使用Fiat-Shamir 变换。我们将所有的随机挑战替换为对某些值的哈希，比如说$y = \mathrm{H}(A,S)$，$Z = \mathrm{H}(A,S,y)$。

同时为了避免一个受信任初始化阶段，我们可以使用一个能够从较小的种子池中产生公共参数$\boldsymbol{g},\boldsymbol{h},g,h$的哈希函数，这个哈希函数应当是一个从$\{0,1\}^*$到$G\setminus\{1\}$的映射。这样的哈希函数可以参考 Dan Boneh 等人在 2001 年发表的论文 [14] 进行构建。

参考文献:

[1] Maxwell,G. Confidential transactions. https://people.xiph. org/~greg/ confidential_values.txt, 2016.

[2] 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]

[3] Bootle J, Cerulli A, Chaidos P, Groth J, Petit C. Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting[C]. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 327–357. Springer, 2016.

[4] G. Maxwell and A. Poelstra. Borromean ring signatures. http://diyhpl. us/~bryan/papers2/bitcoin/Borromean%20ring%20signatures.pdf, 2015.

[5] 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]

[6] 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]

[7] 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

[8] 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

[9] 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]

[10] G Dagher, B B¨unz, Joseph Bonneau, Jeremy Clark, and D Boneh. Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges (full version). Technical report, IACR Cryptology ePrint Archive, 2015.

[11] Andrew Poelstra, Adam Back, Mark Friedenbach, Gregory Maxwell, and Pieter Wuille. Confidential assets.

[12] Jan Camenisch, Rafik Chaabouni, and abhi shelat. Efficient protocols for set membership and range proofs. Advances in Cryptology-ASIACRYPT 2008, pages 234–252, 2008.

[13] Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signature problems[J]. CRYPTO 1986: pp. 186-194.

[14]Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In International Conference on the Theory and Application of Cryptology and Information Security, pages 514–532. Springer, 2001.