ZK SHANGHAI
零知识证明工作坊

PLONK及证明系统技术栈

WORKSHOP!

现代零知识密码学

Hosted by SutuLabs & Kepler42B-ZK Planet

课程资源：zkshanghai.xyz

个人介绍

梁爽

区块链 架构师

上海交大 计算机博士生
（休学创业中）

微信：icerdesign
微博：@wizicer
Github: @wizicer
Twitter: @icerdesign
LinkedIn: www.linkedin.com/in/icerdesign

1999年	• 正式开始学习写程序
2009年	• 在新媒传信（飞信）做高性能服务器程序架构及开发
2012年	• 在Honeywell工业控制部门做PLC、RTU上位机组态软件架构及开发
2017年	• 接触区块链，并开始创业开发区块链数据库
2020年	• 入学上海交大攻读博士学位，研究零知识证明数据库
2022年	• 获Chia全球开发大赛第一名，并开始Pawket钱包的开发
2023年	• 获得零知识链Mina的项目资助

今日课程内容

- 证明系统技术栈
- PLONK

今日课程将回答以下问题

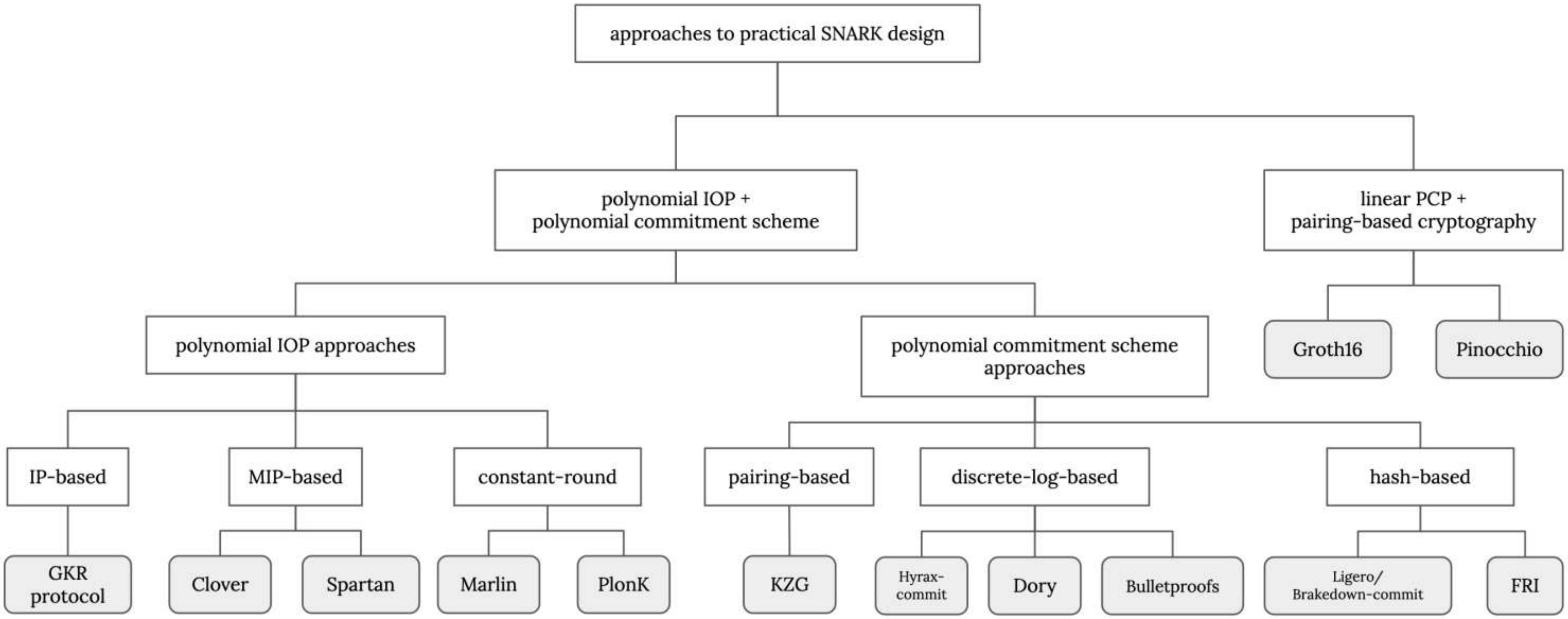
- 过去几节数学课的知识属于证明系统中的位置
- 如何编写PLONK框架

模块化SNARK


算术电路
计算正确性
算术化
约束满足性检查
信息论安全证明
密码学编译器
证明系统


待证明陈述
C-SAT等问题
易证明的语言
信息论安全证明
Information-theoretic proof
密码编译器
简洁非交互零知识证明

证明系统分类


approaches to practical SNARK design
polynomial IOP +
polynomial commitment scheme
linear PCP +
pairing-based cryptography
polynomial IOP approaches
polynomial commitment scheme
approaches
Groth16
Pinocchio
IP-based
MIP-based
constant-round
pairing-based
discrete-log-based
hash-based
GKR
protocol
Clover
Spartan
Marlin
PlonK
KZG
Hyrax-
commit
Dory
Bulletproofs
Ligero/
Brakedown-commit
FRI

LPCP/QAP的零知识证明

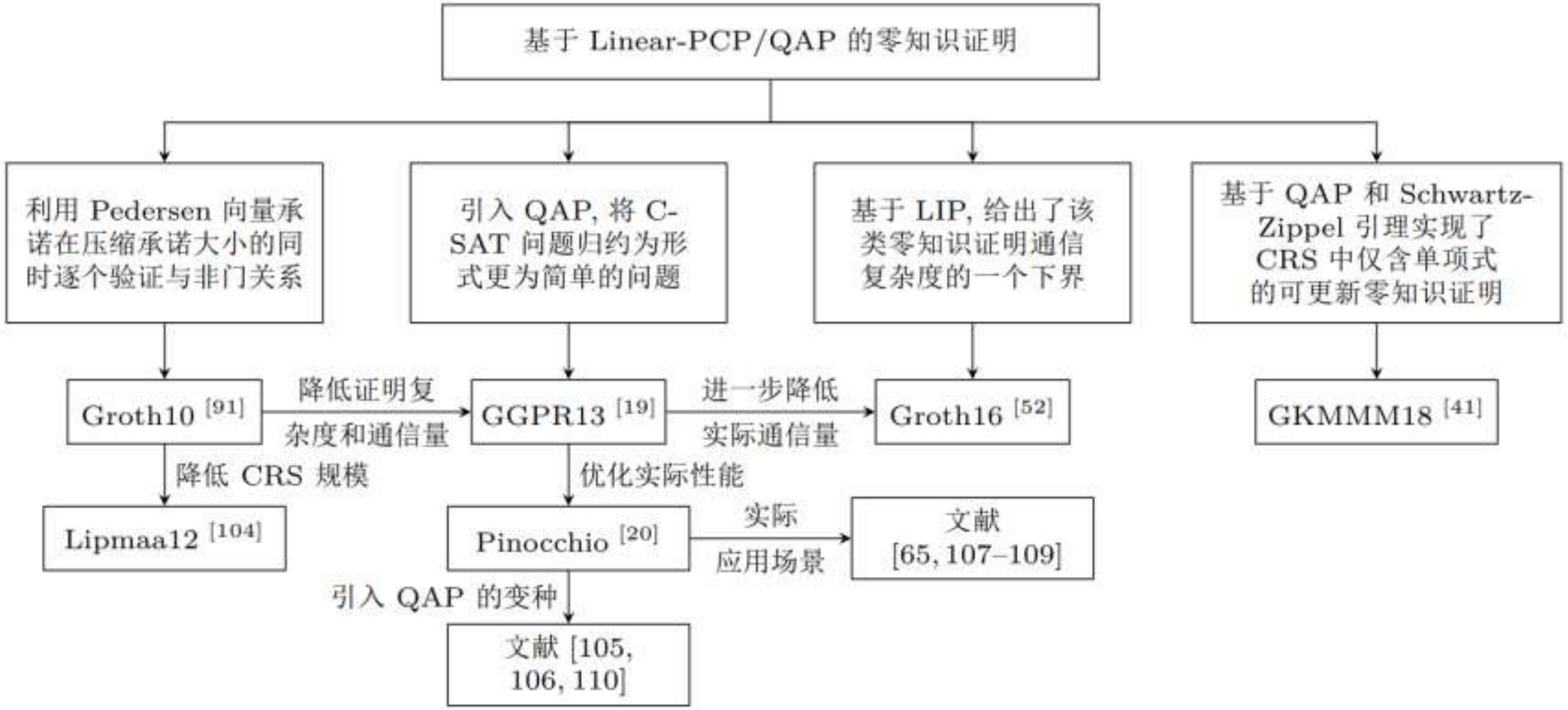
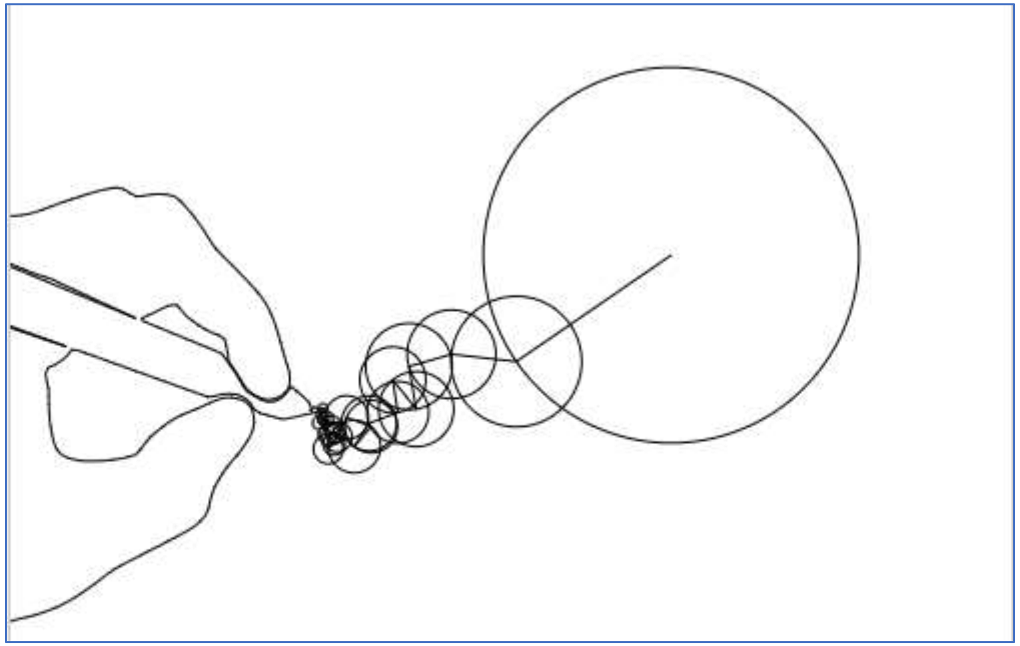


图 5 基于 QAP 的部分零知识证明协议优化思路

Figure 5 Optimization of several zero-knowledge proof based on QAP

李威翰, 张宗洋, 周子博, and 邓燚 2022. 简洁非交互零知识证明综述. 密码学报. 9, 3 (2022), 69.

傅里叶变换



https://www.jezzamon.com/fourier/

- 傅里叶变换可以将一个信号分解成一系列正弦和余弦函数的叠加

离散傅里叶变换(DFT)

- 为了找到特定频率下的能量，将信号在该频率上绕圆圈旋转，并沿着该路径平分一堆点。

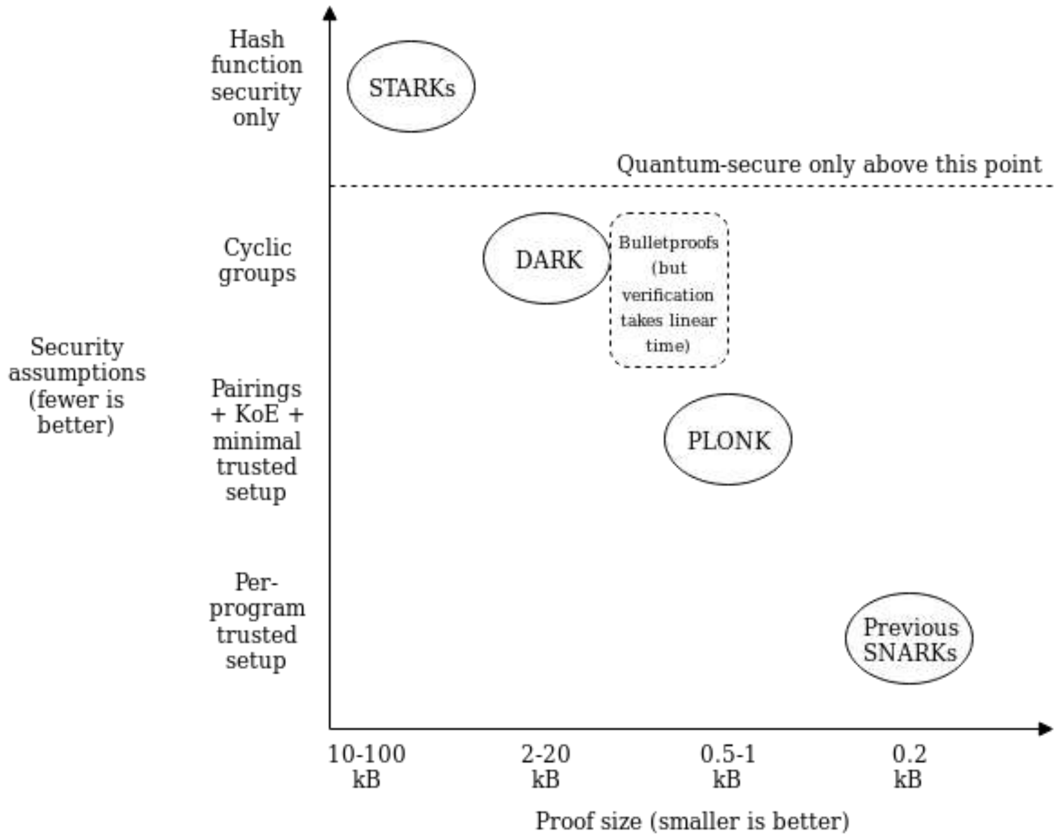
$$X_k = \frac{1}{N}\sum_{n=0}^{N-1} x_n e^{i2\pi k\frac{n}{N}}$$

http://www.altdevblogaday.com/2011/05/17/understanding-the-fourier-transform/

PlonK

Permutations over **L**agrange-bases for **O**ecumenical **N**oninteractive arguments of **K**nowledge

- 利用KZG承诺，可以变为通用设置，即一次仪式可适应不同电路
- 利用FRI或DARK承诺方案，可以变为透明设置



https://vitalik.ca/general/2019/09/22/plonk.html

准备双线性映射的两个群

- 定义有限域
- 寻找G_1的循环子群
- 设置扩展域
- 找到第二个子群G_2

定义有限域

- $y^2 = x^3 + ax + b$
- $x, y \in \mathbb{F}_{101}, a = 0, b = 3$
- $\mathbb{F}_{101}$性质很方便，比如$100 \equiv -1, 50 \equiv -\frac{1}{2}, 20 \equiv -\frac{1}{5}$

寻找G_1的循环子群

- 生成元$G_1 = (1,2)$
- $2G_1 = (68,74), -2G_1 = (68,27)$
- $4G_1 = (65,98), -4G_1 = (65,3)$
- $8G_1 = (18,49), -8G_1 = (18,52)$
- $16G_1 = (1,99), -16G_1 = (1,2)$

- 因此G_1子群的阶为17

- 计算方法
  - 原始点$P = (x, y)$
  - 点翻倍
    - 计算斜率：$s = \frac{3x^2}{2y}$
    - 假设$2P = (\hat{x}, \hat{y})$
    - $\hat{x} = s^2 - 2x$
    - $\hat{y} = s(x - \hat{x}) - y$
  - 点取反
    - $-P = (x, -y)$

扩展域

- 寻找扩展域$\mathbb{F}_{101^k}$
- 嵌入度k
- 找到最小的k，使得$r|p^k-1$
- 例如$k=2$
  - $p^k-1=101^2-1\equiv 0(mod\ 17)$

- 扩展域$\mathbb{F}_{101^2}$
- 寻找一个不可约二次式x^2+2
- u为该式的解，即$u^2=-2$
- 该扩展域所有元素可写作$a+bu$

找到第二个子群

- 生成元$G_2 = (36,31u)$
- 检查从属：
  - $y^2 = x^3 + 3$
  - $(31u)^2 \equiv 36^3 + 3\ (mod\ 101)$
  - $31^2 \cdot u^2 \equiv 98\ (mod\ 101)$
  - $52 \cdot (-2) \equiv 98\ (mod\ 101)$
  - $98 \equiv 98\ (mod\ 101)$

- 计算方法
  - 原始点$P = (x, y)$
  - 点翻倍
    - 计算斜率：$s = \frac{3x^2}{2y}$
    - 假设$2P = (\hat{x}, \hat{y})$
    - $\hat{x} = s^2 - 2x$
    - $\hat{y} = s(x - \hat{x}) - y$

可信设置

- 选取安全数字 s
- 构造结构引用字符串SRS:
  - $1 \cdot G_1,\ s \cdot G_1,\ s^2 \cdot G_1,\ \ldots,\ s^{n+2} \cdot G_1,$
  - $1 \cdot G_2,\ s \cdot G_2$
- 例$s = 2, n = 4$
  - $(1,2), (68,74), (65,98), (18,49), (1,99), (68,27), (65,3),$
  - $(36,31u), (90,82u)$

定义问题陈述（电路设计）

- 勾股数问题： $\alpha^2 + \beta^2 = \gamma^2$
- 数字约束可以简化为

$x_1 \cdot x_1 = x_2$
$x_3 \cdot x_3 = x_4$
$x_5 \cdot x_5 = x_6$
$x_2 + x_4 = x_6$

PLONK基本多项式

$$q_l a + q_r b + q_o c + q_m ab + q_c = 0$$

左输入 右输入 输出 乘法 常数

问题转换为PLONK电路表达

a	b	c	expresion	gate	polynomial
3	3	9	$x_1 \cdot x_1 = x_2$	$a_1 \cdot b_1 = c_1$	$+0a_1 + 0b_1 - 1c_1 + 1a_1b_1 + 0 = 0$
4	4	16	$x_3 \cdot x_3 = x_4$	$a_2 \cdot b_2 = c_2$	$+0a_2 + 0b_2 - 1c_2 + 1a_2b_2 + 0 = 0$
5	5	25	$x_5 \cdot x_5 = x_6$	$a_3 \cdot b_3 = c_3$	$+0a_3 + 0b_3 - 1c_3 + 1a_3b_3 + 0 = 0$
9	16	25	$x_2 + x_4 = x_6$	$a_4 + b_4 = c_4$	$+1a_4 + 1b_4 - 1c_4 + 0a_4b_4 + 0 = 0$

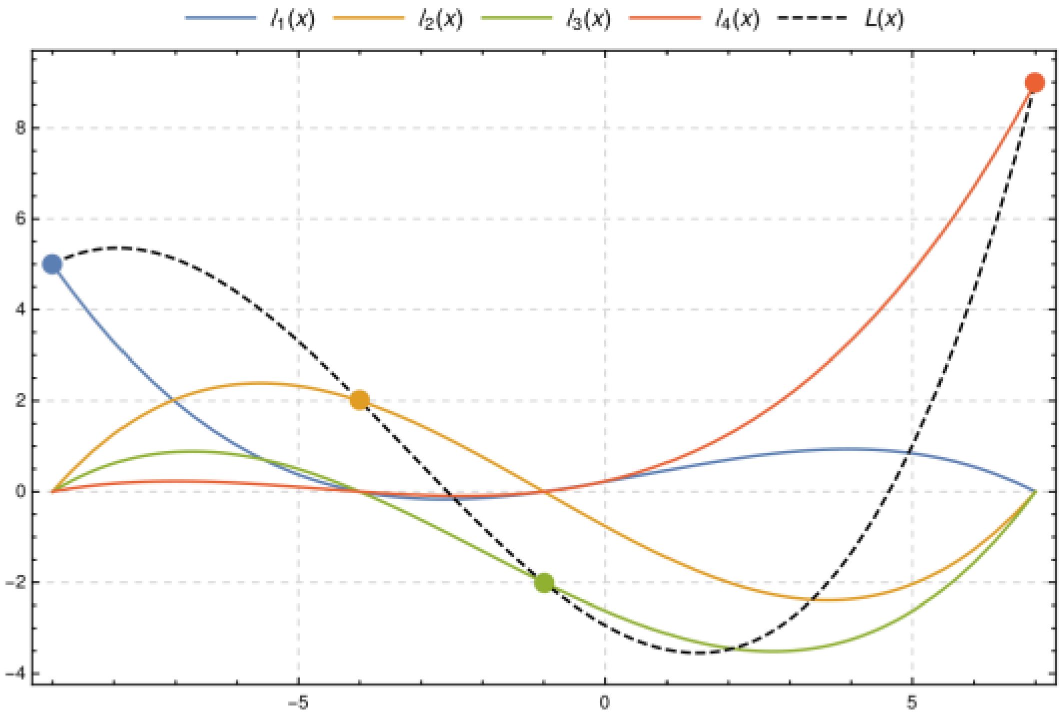
q_l q_r q_o q_m q_c

转换为向量

- $\boldsymbol{q_l} = (0,0,0,1)$
- $\boldsymbol{q_r} = (0,0,0,1)$
- $\boldsymbol{q_o} = (-1,-1,-1,-1)$
- $\boldsymbol{q_m} = (1,1,1,0)$
- $\boldsymbol{q_c} = (0,0,0,0)$
- $\boldsymbol{a} = (3,4,5,9)$
- $\boldsymbol{b} = (3,4,5,16)$
- $\boldsymbol{c} = (9,16,25,25)$

a	b	c	expresion	gate	polynomial
3	3	9	$x_1 \cdot x_1 = x_2$	$a_1 \cdot b_1 = c_1$	$+0a_1 + 0b_1 - 1c_1 + 1a_1b_1 + 0 = 0$
4	4	16	$x_3 \cdot x_3 = x_4$	$a_2 \cdot b_2 = c_2$	$+0a_2 + 0b_2 - 1c_2 + 1a_2b_2 + 0 = 0$
5	5	25	$x_5 \cdot x_5 = x_6$	$a_3 \cdot b_3 = c_3$	$+0a_3 + 0b_3 - 1c_3 + 1a_3b_3 + 0 = 0$
9	16	25	$x_2 + x_4 = x_6$	$a_4 + b_4 = c_4$	$+1a_4 + 1b_4 - 1c_4 + 0a_4b_4 + 0 = 0$

拉格朗日插值(Lagrange Interpolation)



- 该图显示了经过四个点 $((-9,5),(-4,2),(-1,-2),(7,9))$的插值多项式$L(x)$（黑色虚线）
- 它是缩放基本多项式$y_0\ell_0(x)$，$y_1\ell_1(x)$，$y_2\ell_2(x)$和$y_3\ell_3(x)$的和。
- 插值多项式通过所有四个控制点，并且每个缩放基本多项式通过其相应的控制点，并且在x对应于其他三个控制点的位置为0。

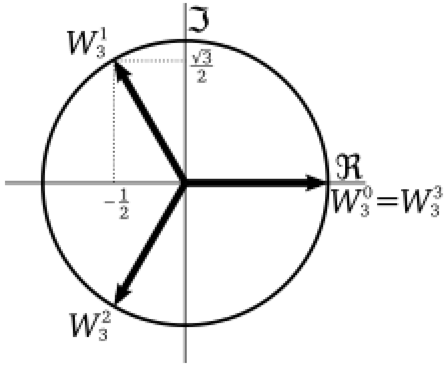
利用拉格朗日插值将向量转换为多项式

- $\boldsymbol{a} = (3,4,5,9)$
- 转换为坐标$(0,3), (1,4), (2,5), (3,9)$
- 穿过这些坐标的拉格朗日多项式：$\frac{1}{2}x^3 - \frac{3}{2}x^2 + 2x + 3 = 0$

单位根

Root of unity

- 称 $x^n = 1$ 在复数意义下的解是 n 次复根。
- 这样的解有 n 个，称这 n 个解都是 n 次 **单位根** 或 **单位复根**（the n-th root of unity）。
- 根据复平面的知识，n 次单位根把单位圆 n 等分。
- n 需要大于等于约束向量的长度。



解出4次单位根

$$H : \{x \in \mathbb{F}_{17} | x^4 = 1\}$$

$$x^4 = 1 \implies x^2 = \pm 1 = 1 \text{ or } 16$$

$$x^2 = 1 \implies x = \pm 1 = 1 \text{ or } 16$$

$$x^2 = 16 \implies x = \pm 4 = 4 \text{ or } 13$$

$$H : \{1, 4, 16, 13\}$$

计算陪集（coset）

$$H : \{1, 4, 16, 13\}$$

$$k_1 = 2, k_2 = 3$$

$$k_1H : \{2, 8, 15, 9\}$$

$$k_2H : \{3, 12, 14, 5\}$$

多项式插值

$$f(x) = a + bx + cx^2 + dx^3$$

$$(a, b, c, d) = \Omega^{-1} \cdot (f(\omega^0), f(\omega^1), f(\omega^2), f(\omega^3))^T$$

$$\Omega^{-1} = \frac{1}{4} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 13 & 16 & 4 \\ 1 & 16 & 1 & 16 \\ 1 & 4 & 16 & 13 \end{bmatrix} = \begin{bmatrix} 13 & 13 & 13 & 13 \\ 13 & 16 & 4 & 1 \\ 13 & 4 & 13 & 4 \\ 13 & 1 & 4 & 16 \end{bmatrix}$$

$$f_a = 1 + 13x + 3x^2 + 3x^3$$

$$f_b = 7 + 3x + 14x^2 + 13x^3$$

$$f_c = 6 + 5x + 11x^2 + 4x^3$$

$$q_L = 13 + x + 4x^2 + 16x^3$$

$$q_R = 13 + x + 4x^2 + 16x^3$$

$$q_O = 16$$

$$q_M = 5 + 16x + 13x^2 + x^3$$

$$q_C = 0$$

拷贝约束

expresion	gate
$x_1 \cdot x_1 = x_2$	$a_1 \cdot b_1 = c_1$
$x_3 \cdot x_3 = x_4$	$a_2 \cdot b_2 = c_2$
$x_5 \cdot x_5 = x_6$	$a_3 \cdot b_3 = c_3$
$x_2 + x_4 = x_6$	$a_4 + b_4 = c_4$

$$a_1 = b_1 = x_1$$
$$a_2 = b_2 = x_2$$
$$a_3 = b_3 = x_3$$
$$a_4 = c_1$$
$$b_4 = c_2$$
$$c_4 = c_3$$

$$a: \quad H: \{1, 4, 16, 13\}$$
$$b: k_1 H: \{2, 8, 15, 9\}$$
$$c: k_2 H: \{3, 12, 14, 5\}$$

$$S_{\sigma_1}(x) = 7 + 13x + 10x^2 + 6x^3$$
$$S_{\sigma_2}(x) = 4 + 13x^2 + x^3$$
$$S_{\sigma_3}(x) = 6 + 7x + 3x^2 + 14x^3$$

证明第一步：承诺 a, b, c （编码赋值）

设 $Z_H(x) = x^4 - 1$，有:

$$
\begin{aligned}
a(x) &= (b_1 x + b_2) \cdot Z_H(x) + f_a(x) \\
b(x) &= (b_3 x + b_4) \cdot Z_H(x) + f_b(x) \\
c(x) &= (b_5 x + b_6) \cdot Z_H(x) + f_c(x)
\end{aligned}
$$

在域 $\mathbb{F}_{17}$ 上生成随机数，假设是 $(b_1, b_2, b_3, b_4, b_5, b_6) = (7, 4, 11, 12, 16, 2)$，则有:

$$
\begin{aligned}
a(x) &= 14 + 6x + 3x^2 + 3x^3 + 4x^4 + 7x^5 \\
b(x) &= 12 + 9x + 14x^2 + 13x^3 + 12x^4 + 11x^5 \\
c(x) &= 4 + 6x + 11x^2 + 4x^3 + 2x^4 + 16x^5
\end{aligned}
$$

我们利用 SRS 进行承诺

$$
\begin{aligned}
[a(x)]_1 &= (91, 66) \\
[b(x)]_1 &= (26, 45) \\
[c(x)]_1 &= (91, 35)
\end{aligned}
$$

证明第二步：承诺 z （编码拷贝约束）

生成随机数 $(b_7, b_8, b_9) = (14, 11, 7) \in \mathbb{F}_{17}$，计算 $z(x)$：

$$z(x) = (b_7 x^2 + b_8 x + b_9) \cdot Z_H(x) + acc(x)$$

根据从验证者得到的挑战 $(\beta, \gamma) = (12, 13) \in \mathbb{F}_{17}$ 计算出累加器向量

$$acc_0 = 1$$

$$acc_i = acc_{i-1} \frac{(a_i + \beta\omega^{i-1} + \gamma)(b_i + \beta k_1 \omega^{i-1} + \gamma)(c_i + \beta k_2 \omega^{i-1} + \gamma)}{(a_i + \beta S_{\sigma_1}(\omega^{i-1}) + \gamma)(b_i + \beta S_{\sigma_2}(\omega^{i-1}) + \gamma)(c_i + \beta S_{\sigma_3}(\omega^{i-1}) + \gamma)}$$

证明第二步：承诺 z

$$acc_1 = 1 \cdot \frac{(3+12*1+13)(3+12*2*1+13)(9+12*3*1+13)}{(3+12*2+13)(3+12*1+13)(9+12*13+13)}$$

$$= \frac{11 \cdot 6 \cdot 7}{6 \cdot 11 \cdot 8} = 3$$

$$acc_2 = 3 \cdot \frac{(4+12*4+13)(4+12*2*4+13)(16+12*3*4+13)}{(4+12*8+13)(4+12*4+13)(16+12*9+13)}$$

$$= 3 \cdot \frac{14 \cdot 11 \cdot 3}{11 \cdot 14 \cdot 1} = 9$$

$$acc_3 = 9 \frac{(5+12*16+13)(5+12*2*16+13)(25+12*3*16+13)}{(5+12*15+13)(5+12*16+13)(25+12*5+13)}$$

$$= 9 \cdot \frac{6 \cdot 11 \cdot 2}{11 \cdot 6 \cdot 13} = 4$$

证明第二步：承诺 z

通过插值得到累加器多项式

$$acc = (1, 3, 9, 4)$$
$$acc(x) = 16x + 5x^2 + 14x^3$$

$$\begin{aligned} z(x) &= (14x^2 + 11x + 7)(x^4 - 1) + 16x + 5x^2 + 14x^3 \\ &= 10 + 5x + 8x^2 + 14x^3 + 7x^4 + 11x^5 + 14x^6 \end{aligned}$$

$$[z(x)]_1 = |z(s)| \cdot G_1 = (32, 59)$$

证明第三步：承诺 t (a, b, c, z)

根据验证者发起的挑战 $\alpha = 15 \in \mathbb{F}_{17}$，计算商多项式

$$
\begin{aligned}
t(x) = &\left(a(x)b(x)q_M(x) + a(x)q_L(x) + b(x)q_R(x) + c(x)q_O(x) + PI(x) + q_C(x)\right)\frac{1}{Z_H(x)} \\
&+ (a(x) + \beta x + \gamma)(b(x) + \beta k_1 x + \gamma)(c(x) + \beta k_2 x + \gamma)z(x)\frac{\alpha}{Z_H(x)} \\
&- (a(x) + \beta S_{\sigma_1}(x) + \gamma)(b(x) + \beta S_{\sigma_2}(x) + \gamma)(c(x) + \beta S_{\sigma_2}(x) + \gamma)z(\omega x)\frac{\alpha}{Z_H(x)} \\
&+ (z(x) - 1)L_1(x)\frac{\alpha^2}{Z_H(x)}
\end{aligned}
$$

分解为度 $< n + 2$ 的多项式 $t_{lo}(x), t_{mid}(x), t_{hi}(x)$ 其中

$$t(x) = t_{lo}(x) + x^{n+2}t_{mid}(x) + x^{2n+4}t_{hi}(x)$$

计算结果：$[t_{lo}(x)]_1, [t_{mid}(x)]_1, [t_{hi}(x)]_1$.

证明第三步：承诺 t （a, b, c, z）

$$t(x) = 11x^{17} + 7x^{16} + 2x^{15} + 16x^{14} + 6 * x^{13} + 15x^{12} + x^{11} + 10x^{10} + 2x^{9} + x^{8} + 8x^{7} + 13x^{6} + 13x^{5} + 9x^{3} + 13x^{2} + 16x + 11$$

$$\begin{aligned} t_{lo} &= 11 + 16x + 13x^2 + 9x^3 + 13x^5 \\ t_{mid} &= 13 + 8x + x^2 + 2x^3 + 10x^4 + x^5 \\ t_{hi} &= 15 + 6x + 16x^2 + 2x^3 + 7x^4 + 11x^5 \end{aligned}$$

承诺结果：

$$\begin{aligned} [t_{lo}]_1 &= (12, 32) \\ [t_{mid}]_1 &= (26, 45) \\ [t_{hi}]_1 &= (91, 66) \end{aligned}$$

证明第四步：承诺 r （用评估点替换 t 内容）

计算打开评估

$$\bar{a}=a(\zeta),\bar{b}=b(\zeta),\bar{c}=c(\zeta),\bar{S_{\sigma_1}}=S_{\sigma_1}(\zeta),\bar{S_{\sigma_2}}=S_{\sigma_2}(\zeta),\bar{t}=t(\zeta),\bar{z_\omega}=z(\omega\zeta)$$

计算线性化多项式（关于承诺值的线性多项式）：

$$\begin{aligned}r(x)=&\ \bar{a}\bar{b}q_m(x)+\bar{a}q_l(x)+\bar{b}q_r(x)+\bar{c}q_o(x)+q_c(x)\\&+\alpha(\bar{a}+\beta\zeta+\gamma)(\bar{b}+\beta k_1\zeta+\gamma)(\bar{c}+\beta k_2\zeta+\gamma)z(x)\\&-\alpha(\bar{a}+\beta\bar{S_{\sigma_1}}+\gamma)(\bar{b}+\beta\bar{S_{\sigma_2}}+\gamma)\beta\bar{z_\omega}S_{\sigma_3}(x)\\&+\alpha^2z(x)L_1(\zeta)\end{aligned}$$

$r(x)$的定义与Plonk论文中不同，在进行线性化时，我们删除了所有常数项。这可以节省一个验证者标量乘法。

计算线性化评估$\bar{r}=r(\zeta)$。并输出

$$\bar{a},\bar{b},\bar{c},\bar{S_{\sigma_1}},\bar{S_{\sigma_2}},\bar{z_\omega},\bar{t},\bar{r}$$

假设$\zeta=5$，则有：（计算过程略）

$$\bar{a}=15,\bar{b}=13,\bar{c}=5,\bar{S_{\sigma_1}}=1,\bar{S_{\sigma_2}}=12,\bar{t}=1,\bar{z_\omega}=15,\bar{r}=15$$

证明第五步：承诺所有

计算打开挑战 $v \in \mathbb{F}_{17}$

计算打开证明多项式 $W_\zeta(x)$:

$$W_\zeta(x) = \frac{1}{x-\zeta} \cdot \begin{bmatrix} t_{lo}(x) + \zeta^{n+2} t_{mid}(x) + \zeta^{2n+4} t_{hi}(x) - \bar{t} \\ +v(r(x) - \bar{r}) \\ +v^2(a(x) - \bar{a}) \\ +v^3(b(x) - \bar{b}) \\ +v^4(c(x) - \bar{c}) \\ +v^5(S_{\sigma_1}(x) - \bar{S_{\sigma_1}}) \\ +v^6(S_{\sigma_2}(x) - \bar{S_{\sigma_2}}) \end{bmatrix}$$

计算打开证明多项式 $W_{\zeta\omega}(x)$:

$$W_{\zeta\omega}(x) = \frac{z(x) - \bar{z_\omega}}{x - \zeta\omega}$$

输出

$$[W_\zeta(x)]_1, [W_{\zeta\omega}(x)]_1$$

设 $\zeta = 5$，则有 $[W_\zeta(x)]_1 = (91, 35), [W_{\zeta\omega}(x)]_1 = (65, 98)$

证明完成：输出证据

证据：

$$\pi = ([a], [b], [c], [z], [t_{lo}], [t_{mid}], [t_{hi}], [W_\zeta], [W_{\zeta\omega}], \bar{a}, \bar{b}, \bar{c}, \bar{S_{\sigma_1}}, \bar{S_{\sigma_2}}, \bar{z_\omega}, \bar{r})$$

具体值是：

$$\pi = ((91, 66), (26, 45), (91, 35), (32, 59), (12, 32), (26, 45), (91, 66), (91, 35), (65, 98), \\ 15, 13, 5, 1, 12, 15, 15)$$

验证者：预处理

利用SRS做预处理

$$
\begin{aligned}
[q_M] &= [q_M(s)] && = 12(1,2) = (12,69) \\
[q_L] &= [q_L(s)] && = 6(1,2) = (32,42) \\
[q_R] &= [q_R(s)] && = 6(1,2) = (32,42) \\
[q_O] &= [q_O(s)] && = 16(1,2) = (1,99) \\
[q_C] &= [q_C(s)] && = 0(1,2) = \infty \\
[S_{\sigma_1}] &= [S_{\sigma_1}(s)] && = 2(1,2) = (68,74) \\
[S_{\sigma_2}] &= [S_{\sigma_2}(s)] && = 13(1,2) = (65,3) \\
[S_{\sigma_3}] &= [S_{\sigma_3}(s)] && = 8(1,2) = (18,49)
\end{aligned}
$$

验证者：验证算法

1. 验证 $[a],[b],[c],[z],[t_{lo}],[t_{mid}],[t_{hi}],[W_\zeta],[W_{\zeta\omega}] \in G_1$。
2. 验证 $\bar{a},\bar{b},\bar{c},\bar{S_{\sigma 1}},\bar{S_{\sigma 2}},\bar{z_\omega},\bar{r} \in \mathbb{F}_{17}$。
3. 验证 $w_{i\in[l]} \in \mathbb{F}_{17}$ （公共输入）。
4. 计算零多项式的评估：$Z_H(\zeta)=\zeta^n-1$。
5. 计算 $L_1(\zeta)=\frac{\zeta^n-1}{n(\zeta-1)}$。
6. 计算公共输入多项式的评估：$PI(\zeta)=\sum_{i\in[l]} w_i L_i(\zeta)$。
7. 计算商多项式的评估：

$$\bar{t}=\frac{\bar{r}+PI(\zeta)-(\bar{a}+\beta\bar{S_{\sigma_1}}+\gamma)(\bar{b}+\beta\bar{S_{\sigma_2}}+\gamma)(\bar{c}+\gamma)\alpha-L_1(\zeta)\alpha^2}{Z_H(\zeta)}$$

验证者：验证算法

8. 计算批量多项式承诺的第一部分。定义 $[D] = v[r(x)] + u[z]$：

$$
\begin{aligned}
[D] &= \bar{a}\bar{b}v[q_M] + \bar{a}v[q_L] + \bar{b}v[q_R] + \bar{c}v[q_O] + v[q_C] \\
&+ ((\bar{a} + \beta\zeta + \gamma)(\bar{b} + \beta k_1\zeta + \gamma)(\bar{c} + \beta k_2\zeta + \gamma)\alpha v + L_1(\zeta)\alpha^2 v + u)[z] \\
&- (\bar{a} + \beta\bar{S}_{\sigma_1} + \gamma)(\bar{b} + \beta S_{\sigma_2} + \gamma)\alpha v\beta\bar{z_\omega}[S_{\sigma_3}]
\end{aligned}
$$

9. 计算完整的批量多项式承诺

$$[F] = [t_{lo}] + \zeta^{n+2}[t_{mid}] + \zeta^{2n+4}[t_{hi}] + [D] + v^2[a] + v^3[b] + v^4[c] + v^5[S_{\sigma_1}] + v^6[S_{\sigma_2}]$$

10. 计算群编码的批量评估 $[E]$：

$$[E] = (\bar{t} + v\bar{r} + v^2\bar{a} + v^3\bar{b} + v^4\bar{c} + v^5\bar{S}_{\sigma_1} + v^6\bar{S}_{\sigma_2} + u\bar{z_\omega}) \cdot [1]$$

11. 批量验证所有评估:

$$e([W_\zeta] + u[W_{\zeta\omega}], [s]_2) = e(\zeta[W_\zeta] + u\zeta\omega[W_{\zeta\omega}] + [F] - [E], [1]_2)$$