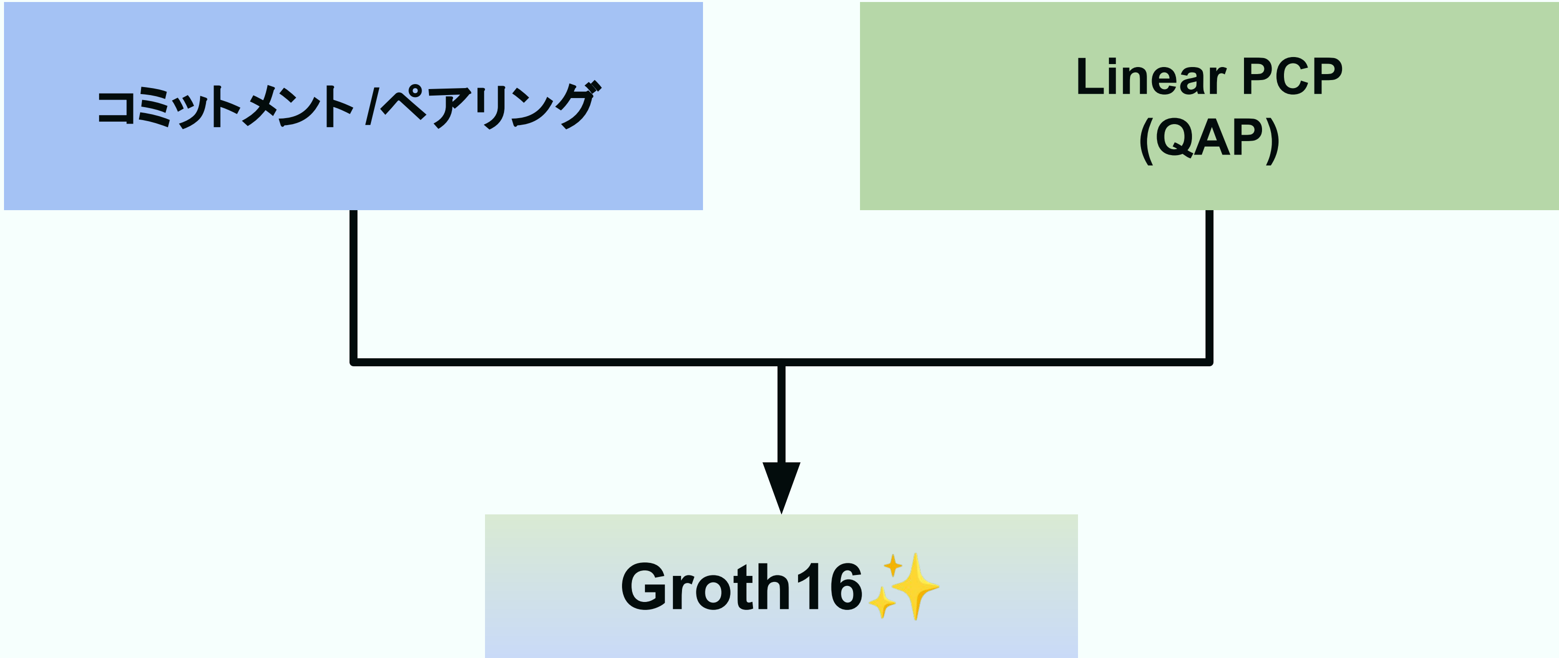
Core Program Week 2

Groth16

ZK Tokyo

Groth16の構成



SNARKの種類

暗号プリミティブ	セットアップ	スキーム
ペアリング	Trusted	Plonk, IP, **Linear PCP (Groth16)**
離散対数	Transparent	Bulletproofs, Dory, Dark, Hyrax, Halo2
ハッシュ	Transparent	STARK, Aurora, Fractal, Virgo, Plonky3

Linear PCPベースSNARKの特徴

✅ 短くて回路長に依存しない証明サイズ（100~200B)

✅ 高速な検証

❌ 線形の証明時間（FFT)

❌ 回路ごとの Trusted Setup

Linear PCPの歴史

PCPが重くて非実用的…

$O(n^2)$の証明時間に！

Kilian'92
PCPとマークルツリー

→

Micali'00
Fiat-Shamir変換を適用

→

IKO'07
Linear PCPと準同型暗号

→

Groth'10
Linear PCPとペアリング

→

Lipmaa'12
gpサイズを削減

→

<u>**GGPR'13**</u>
QSP/QAP

O(nlogn)の証明時間に！

→ SBVBPW13, PGHR13, BCGTV13, BFRSBW13, BCTV14a, BCTV14b, BCGGMTV14, Groth16, SMBW12, SVPBBW12, BCIOP13, ...

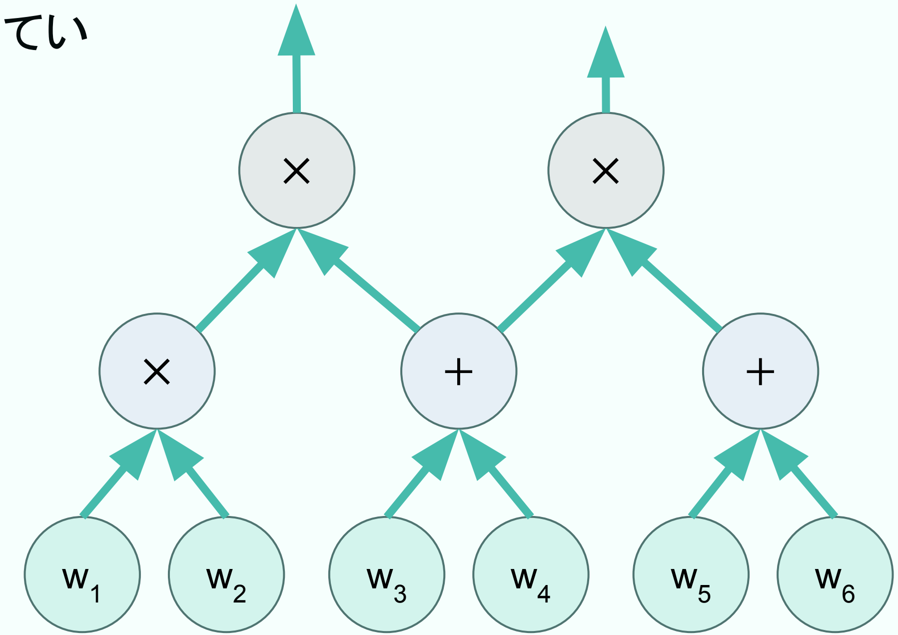
目次

- Quadratic Arithmetic Program (QAP)
- Linear PCP
- Linear PCPによるSNARK
- Groth16

Quadratic Arithmetic Program (QAP)

おさらい: 回路充足性の SNARK

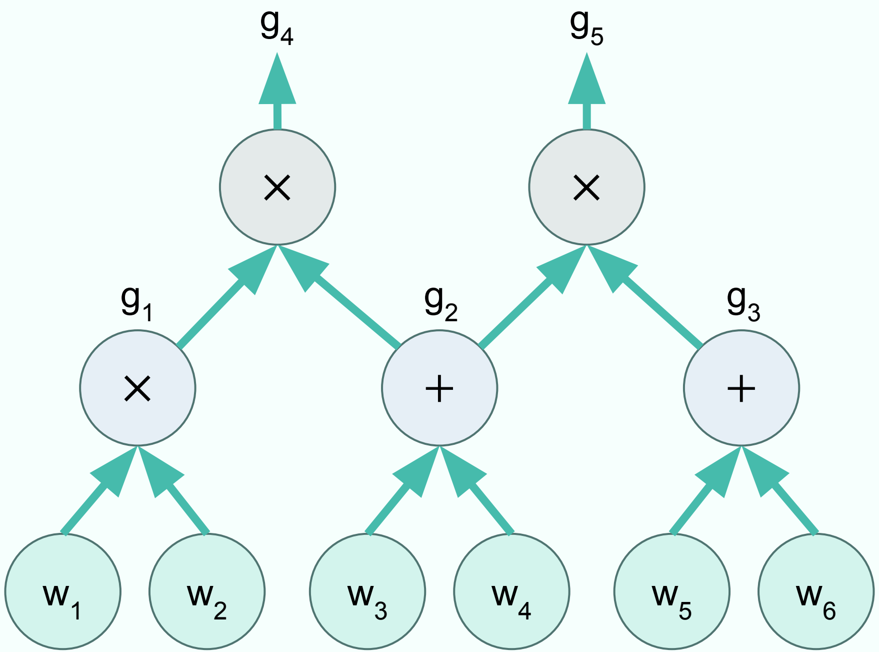
- 算術回路 C(x,w) = y
- 証明者は「C(x,w) = yを満たすwを知っている」ことを主張



QAPの流れ

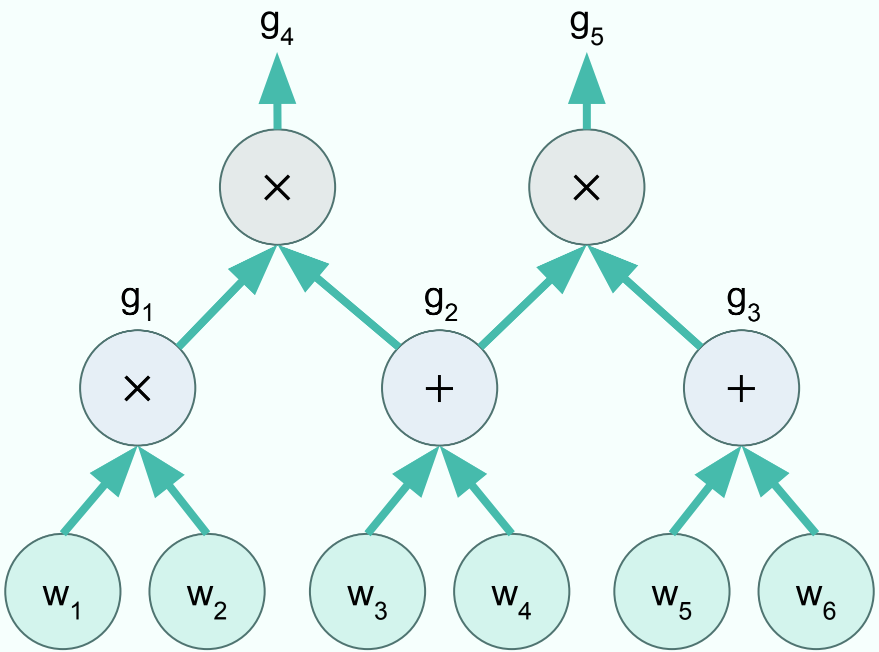
回路 → トレース → セレクター多項式 li(x),ri(x),oi(x) → マスター多項式 p(x)

回路Cのトレース



Interactive Proof 全てのゲートの値	**Plonk** Left input, right input, output	**QAP** Input, 乗算ゲートのoutput
w_1 w_2 w_3 w_4 w_5 w_6 g_1 g_2 g_3 g_4 g_5	w_1 w_2 g_1 w_3 w_4 g_2 w_5 w_6 g_3 g_1 g_2 g_4 g_2 g_3 g_5	? ? ? ? ? ? ? ? ?

回路Cのトレース

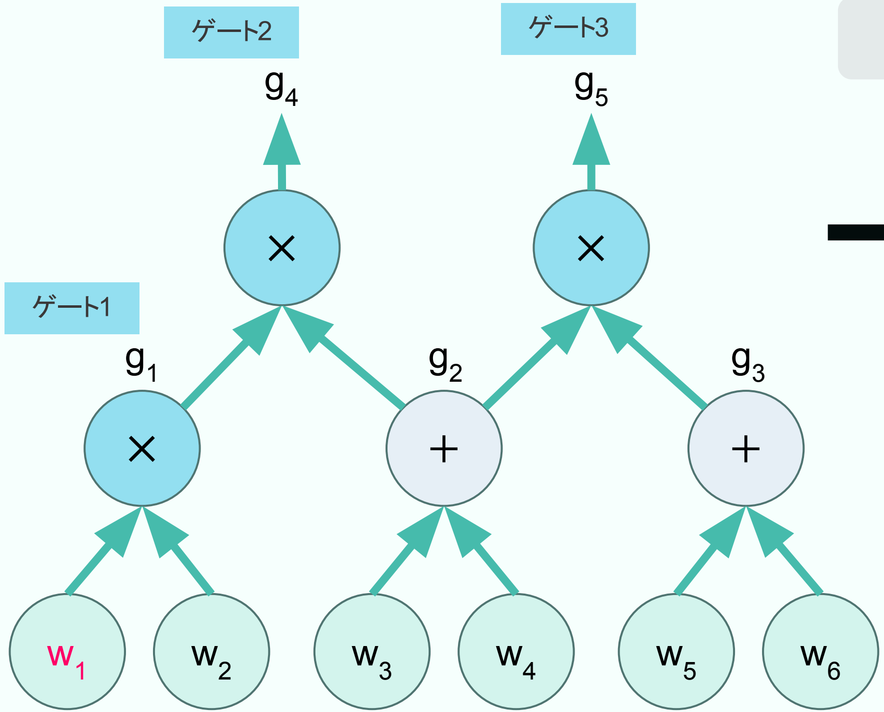


Interactive Proof 全てのゲートの値	**Plonk** Left input, right input, output	**QAP** Input, 乗算ゲートのoutput
w_1, w_2, w_3, w_4, w_5, w_6, g_1, g_2, g_3, g_4, g_5	see table below	w_1, w_2, w_3, w_4, w_5, w_6, g_1, g_4, g_5

Plonk:

w_1	w_2	g_1
w_3	w_4	g_2
w_5	w_6	g_3
g_1	g_2	g_4
g_2	g_3	g_5

セレクター多項式 li



W1がゲートiのleft inputなら1, そうでないなら0

		ω	ω^2	ω^3
c_1	w_1	1	0	0

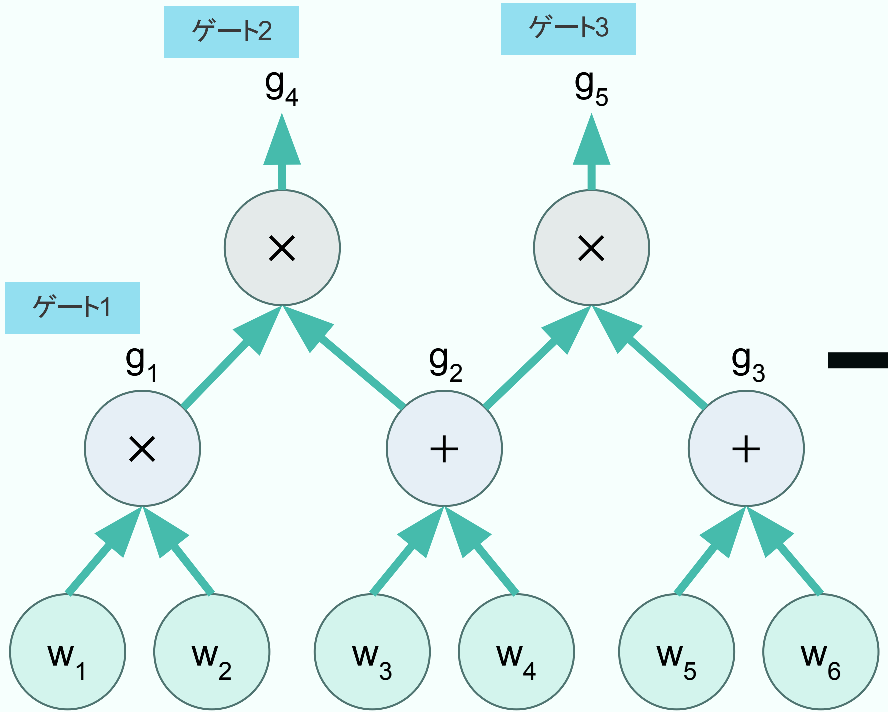
$l1(\omega)=1$, $l1(\omega^2)=0$, $l1(\omega^3)=0$となる多項式l1を構築

有限体$\mathbf{F}_7$で$\omega=2$とおいたときの例

$l1(x) = 3x^2 + 6x + 5 \pmod 7$

セレクター多項式 li: ciがゲートの left inputかどうか

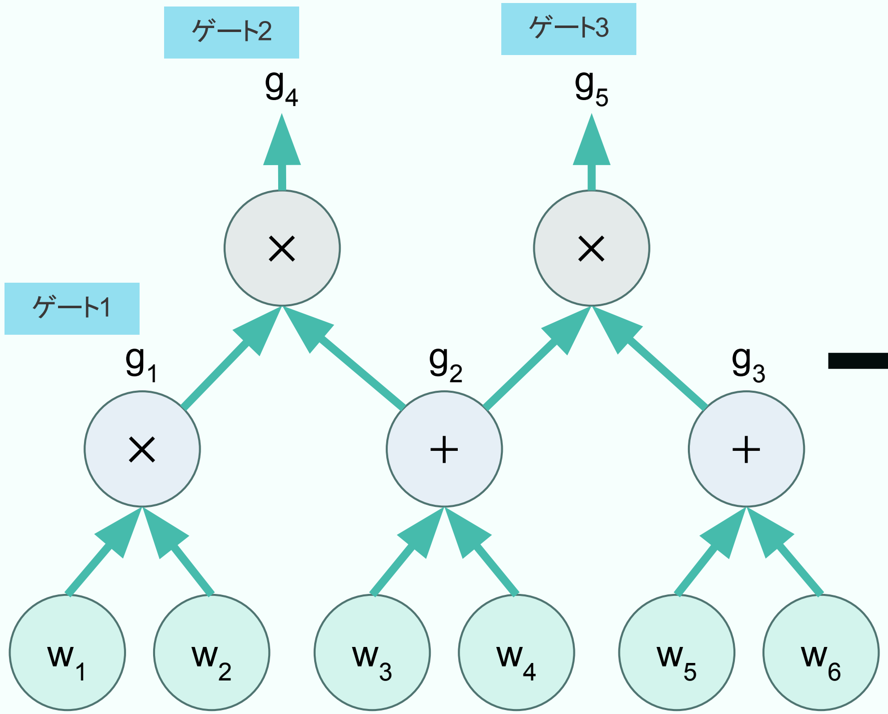
乗算ゲートの前が加算ゲートの場合その inputが1



		ω	ω^2	ω^3	
c_1	w_1	1	0	0	$l_1(x)$
c_2	w_2	?	?	?	$l_2(x)$
c_3	w_3	?	?	?	$l_3(x)$
c_4	w_4	?	?	?	$l_4(x)$
c_5	w_5	?	?	?	$l_5(x)$
c_6	w_6	?	?	?	$l_6(x)$
c_7	g_1	?	?	?	$l_7(x)$
c_8	g_4	?	?	?	$l_8(x)$
c_9	g_5	?	?	?	$l_9(x)$

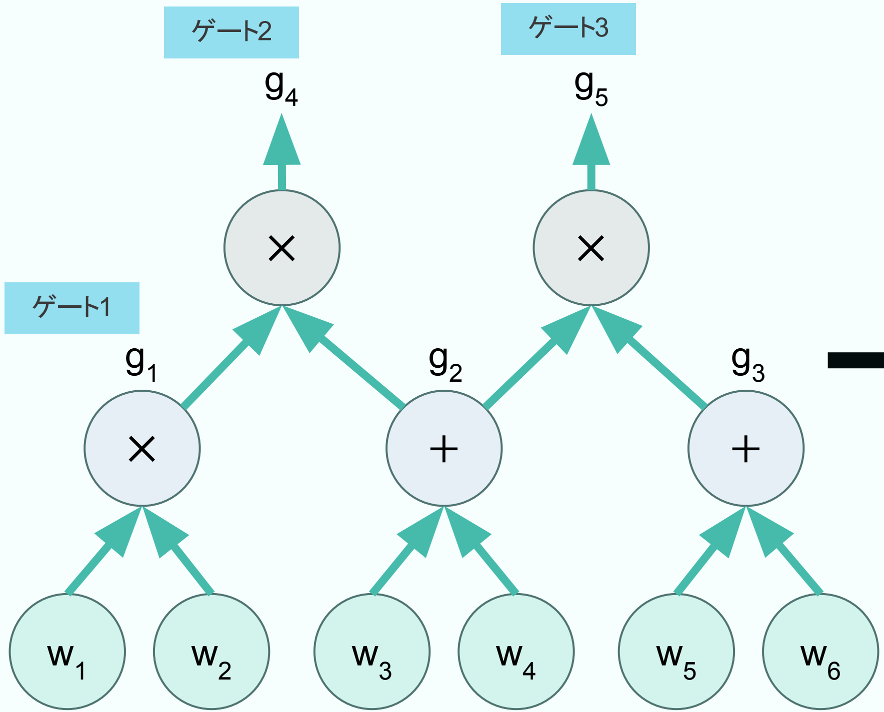
セレクター多項式 li: ciがゲートの left inputかどうか

乗算ゲートの前が加算ゲートの場合その inputが1



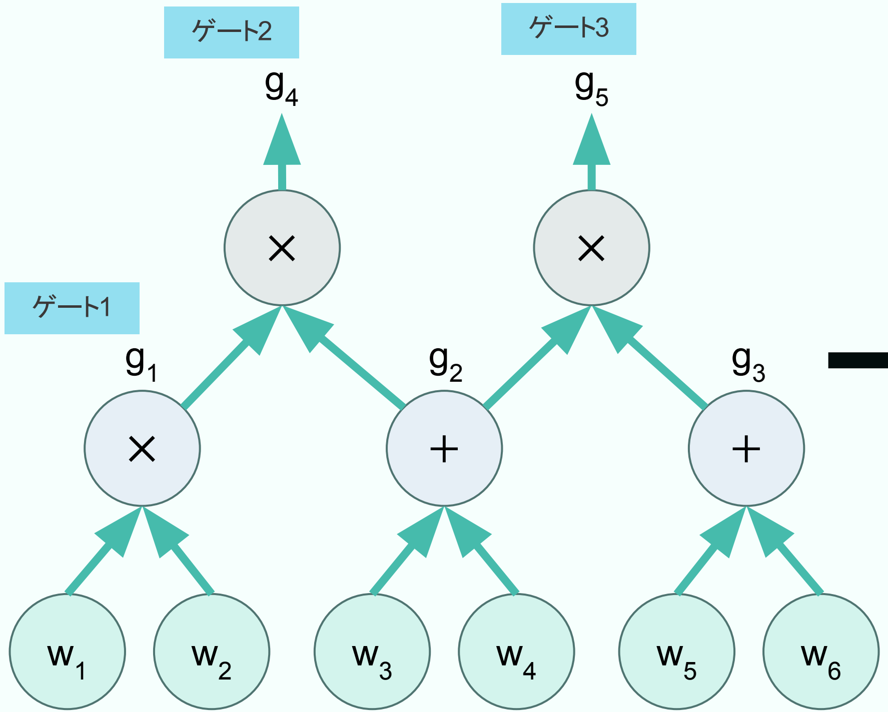
		ω	ω^2	ω^3	
c_1	w_1	1	0	0	l1(x)
c_2	w_2	0	0	0	l2(x)
c_3	w_3	0	0	1	l3(x)
c_4	w_4	0	0	1	l4(x)
c_5	w_5	0	0	0	l5(x)
c_6	w_6	0	0	0	l6(x)
c_7	g_1	0	1	0	l7(x)
c_8	g_4	0	0	0	l8(x)
c_9	g_5	0	0	0	l9(x)

セレクター多項式 ri: ciがゲートの right inputかどうか



		ω	ω^2	ω^3	
c_1	w_1	0	0	0	$r1(x)$
c_2	w_2	1	0	0	$r2(x)$
c_3	w_3	0	1	0	$r3(x)$
c_4	w_4	0	1	0	$r4(x)$
c_5	w_5	0	0	1	$r5(x)$
c_6	w_6	0	0	1	$r6(x)$
c_7	g_1	0	0	0	$r7(x)$
c_8	g_4	0	0	0	$r8(x)$
c_9	g_5	0	0	0	$r9(x)$

セレクター多項式 oi: ciがゲートの outputかどうか



		ω	ω^2	ω^3	
c_1	w_1	0	0	0	o1(x)
c_2	w_2	0	0	0	o2(x)
c_3	w_3	0	0	0	o3(x)
c_4	w_4	0	0	0	o4(x)
c_5	w_5	0	0	0	o5(x)
c_6	w_6	0	0	0	o6(x)
c_7	g_1	1	0	0	o7(x)
c_8	g_4	0	1	0	o8(x)
c_9	g_5	0	0	1	o9(x)

セレクター多項式の例（F7, ω=2）

mod 7	li(x)	ri(x)	oi(x)
w_1	$3x^2 + 6x + 5$	0	0
w_2	0	?	0
w_3	$5x^2 + 5x + 5$	?	0
w_4	$5x^2 + 5x + 5$	?	0
w_5	0	?	0
w_6	0	?	0
g_1	$6x^2 + 3x + 5$	0	?
g_4	0	0	?
g_5	0	0	?

セレクター多項式の例（F7, ω=2）

mod 7	li(x)	ri(x)	oi(x)
w_1	$3x^2 + 6x + 5$	0	0
w_2	0	$3x^2 + 6x + 5$	0
w_3	$5x^2 + 5x + 5$	$6x^2 + 3x + 5$	0
w_4	$5x^2 + 5x + 5$	$6x^2 + 3x + 5$	0
w_5	0	$5x^2 + 5x + 5$	0
w_6	0	$5x^2 + 5x + 5$	0
g_1	$6x^2 + 3x + 5$	0	$3x^2 + 6x + 5$
g_4	0	0	$6x^2 + 3x + 5$
g_5	0	0	$5x^2 + 5x + 5$

マスター多項式 p(x)

$$p(x) = L(x)R(x) - O(x)$$

$$= \left(\sum_{i=1}^{9} c_i \times l_i(x)\right) \times \left(\sum_{i=1}^{9} c_i \times r_i(x)\right) - \left(\sum_{i=1}^{9} c_i \times o_i(x)\right)$$

証明者の主張 : $p(\omega)=0$, $p(\omega^2)=0$, $p(\omega^3)=0$

消失多項式 V(x)

$$p(x) = L(x)R(x) - O(x)$$
$$= \left(\sum_{i=1}^{9} c_i \times l_i(x)\right) \times \left(\sum_{i=1}^{9} c_i \times r_i(x)\right) - \left(\sum_{i=1}^{9} c_i \times o_i(x)\right)$$

$$p(x) = V(x)q(x)$$

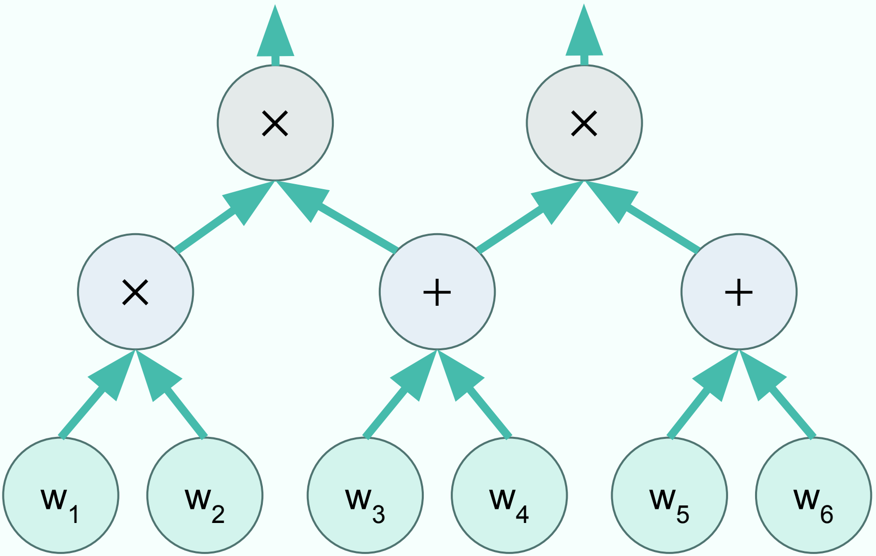
これを満たす多項式qが
存在する！

$$V(x) = (x - \omega)\left(x - \omega^2\right)\left(x - \omega^3\right)$$

回路充足性から QAPへ

証明者の主張：
C(x,w)=yを満たすwを知っている

証明者の主張：
p(x)=V(x)q(x)となるqを知っている



$$p\left(x\right)=V\left(x\right)q\left(x\right)$$

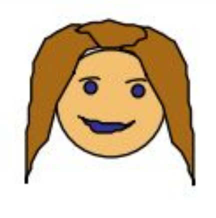
$$=\left(\sum_{i=1}^{9}c_i\times l_i\left(x\right)\right)\times\left(\sum_{i=1}^{9}c_i\times r_i\left(x\right)\right)-\left(\sum_{i=1}^{9}c_i\times o_i\left(x\right)\right)$$

Linear PCP

Probabilistically Checkable Proof (PCP) オラクル

- 一部のポイントだけを確率的に検証するオラクル

i	0	1	2	3	4	5	6	7	8	9
	10	20	50	100	35	40	32	87	92	20

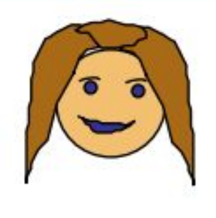


Index 3,5,7の値だけ検証して

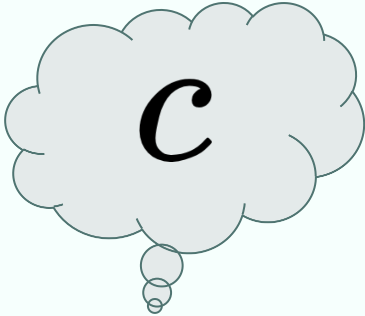
OK

Linear PCP オラクル

- 線形関数の評価結果を検証するPCPオラクル



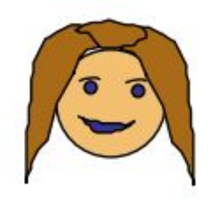
線形関数の結果
<c,q>を教えて



5235414

QAPとLinear PCP オラクル

$$p(x) = \left(\sum_{i=1}^{m} \boxed{c_i} \times l_i\right) \times \left(\sum_{i=1}^{m} \boxed{c_i} \times r_i\right) - \left(\sum_{i=1}^{m} \boxed{c_i} \times o_i\right) = V(x)\boxed{q(x)}$$



$$< c, l_i(\gamma) > \times < c, r_i(\gamma) >$$
$$- < c, o_i(\gamma) > = V(\gamma) < q, \gamma >$$

$$c \quad q(x)$$

9644251

Linear PCPによるSNARK

セットアップ

$$p(x) = \left(\sum c_i \times l_i(x)\right) \times \left(\sum c_i \times r_i(x)\right) - \left(\sum c_i \times o_i(x)\right) = V(x)q(x)$$

PK

$p, \mathbb{G}, g, \mathbb{G}_T, e$

$g^{l_i(\tau)}, g^{r_i(\tau)}, g^{o_i(\tau)}, g^{\tau^i}$

$(\forall i = 1, \ldots, m)$

VK

$g, g^{V(\tau)}$

この時点でクエリを確定
τが証明者にバレたら
偽の証明をつくれてしまう

証明生成

$$p(x) = \underbrace{\left(\sum c_i \times l_i(x)\right)}_{①} \times \underbrace{\left(\sum c_i \times r_i(x)\right)}_{②} - \underbrace{\left(\sum c_i \times o_i(x)\right)}_{③} = V(x)\underbrace{q(x)}_{④}$$

PK

$p, \mathbb{G}, g, \mathbb{G}_T, e$

$g^{l_i(\tau)}, g^{r_i(\tau)}, g^{o_i(\tau)}, g^{\tau^i}$

$(\forall i = 1, \ldots, m)$

$$\pi_1 = g^{???}$$

$$\pi_2 = g^{???}$$

$$\pi_3 = g^{???}$$

$$\pi_4 = g^{???}$$

証明生成

$$p(x) = \underbrace{\left(\sum c_i \times l_i(x)\right)}_{①} \times \underbrace{\left(\sum c_i \times r_i(x)\right)}_{②} - \underbrace{\left(\sum c_i \times o_i(x)\right)}_{③} = V(x)\underbrace{q(x)}_{④}$$

PK

$p, \mathbb{G}, g, \mathbb{G}_T, e$

$g^{l_i(\tau)}, g^{r_i(\tau)}, g^{o_i(\tau)}, g^{\tau^i}$

$(\forall i = 1, \ldots, m)$

$$\pi_1 = g^{\left(\sum_{i=1}^{m} c \times l_i(\tau)\right)}$$

$$\pi_2 = g^{\left(\sum_{i=1}^{m} c \times r_i(\tau)\right)}$$

$$\pi_3 = g^{\left(\sum_{i=1}^{m} c \times o_i(\tau)\right)}$$

$$\pi_4 = g^{q(\tau)}$$

検証

$$p(x) = \left(\sum c_i \times l_i(x)\right) \times \left(\sum c_i \times r_i(x)\right) - \left(\sum c_i \times o_i(x)\right) = V(x)q(x)$$

VK

$g, g^{V(\tau)}$

$$\frac{e(\pi_1, \pi_2)}{e(\pi_3, g)} \stackrel{?}{=} e\left(g^{V(\tau)}, \pi_4\right)$$

$g^{l_i(\tau)}, g^{r_i(\tau)}, g^{o_i(\tau)}, c_i$ が本当に π の計算に使われてることはどうやって証明すればいい？？？

PK

$p, \mathbb{G}, g, \mathbb{G}_T, e$

$g^{l_i(\tau)}, g^{r_i(\tau)}, g^{o_i(\tau)}, g^{\tau^i}$

$g^\beta, g^{\beta(l_i(\tau)+r_i(\tau)+o_i(\tau))}$

$(\forall i = 1, \ldots, m)$

$$\pi_1 = g^{\sum c_i \times l_i(\tau)}$$

$$\pi_2 = g^{\sum c_i \times r_i(\tau)}$$

$$\pi_3 = g^{\sum c_i \times o_i(\tau)}$$

$$\pi_4 = g^{q(\tau)}$$

$$\pi_5 = \prod \left(g^{\beta(l_i(\tau)+r_i(\tau)+o_i(\tau))}\right)^{c_i}$$

VK

$g, g^{V(\tau)}, g^\beta$

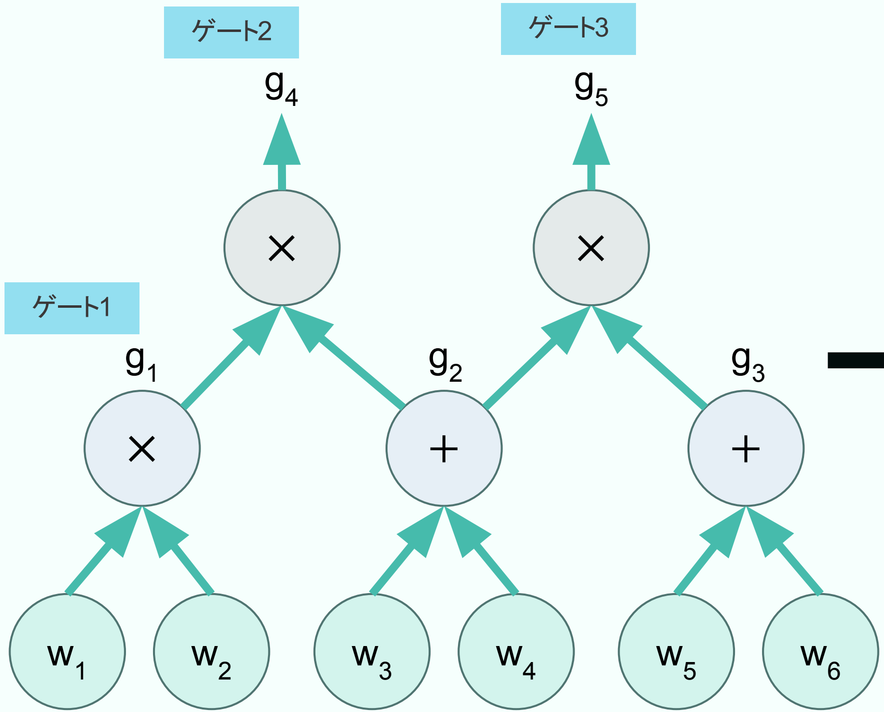
$$\frac{e(\pi_1, \pi_2)}{e(\pi_3, g)} \stackrel{?}{=} e\left(g^{V(\tau)}, \pi_4\right)$$

$$e\left(\pi_1\pi_2\pi_3, g^\beta\right) = e(\pi_5, g)$$

Prover → Verifier

Groth16

Rank-1 Constraint System (R1CS)



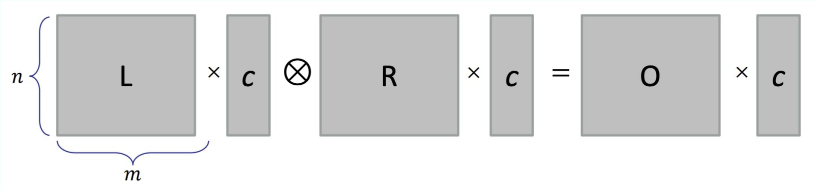
QAPはゲートごとに記述
R1CSは制約ごとに行列形式で記述

QAP

$w_1 \times w_2 - g_1 = 0$

R1CS

$(3w_1 + 5w_5 - 7g_1) \times (6w_2 + 10g_5) - (w_3 - 2g_4) = 0$



Groth16

$$p(x) = \left(\sum c_i \times l_i(x)\right) \times \left(\sum c_i \times r_i(x)\right) - \left(\sum c_i \times o_i(x)\right) = V(x)q(x)$$

PK

$p, \mathbb{G}, g, \mathbb{G}_T, e$

$g^{l_i(\tau)}, g^{r_i(\tau)}, g^{o_i(\tau)}, g^{\tau^i}$

$g^{\alpha}, g^{\beta}, g^{(\beta l_i(\tau)+\alpha r_i(\tau)+o_i(\tau))}$

$(\forall i = 1, \dots, m)$

$$\pi_1 = g^{\alpha + \sum c_i \times l_i(\tau)}$$

$$\pi_2 = g^{\beta + \sum c_i \times r_i(\tau)}$$

$$\pi_3 = g^{\sum c_i \times (\beta l_i(\tau) + \alpha r_i(\tau) + o_i(\tau)) + V(\tau)q(\tau)}$$

VK

g, g^{α}, g^{β}

$$\frac{e(\pi_1, \pi_2)}{e(\pi_3, g)} \stackrel{?}{=} e(g^{\alpha}, g^{\beta})$$

Prover → Verifier

m: mul gateの数

ゼロ知識の達成

$$p(x) = \left(\sum c_i \times l_i(x)\right) \times \left(\sum c_i \times r_i(x)\right) - \left(\sum c_i \times o_i(x)\right) = V(x)q(x)$$

$$\pi_1 = g^{\sum c_i \times l_i(\tau)}$$

$$\pi_2 = g^{\sum c_i \times r_i(\tau)}$$

$$\pi_3 = g^{\sum c_i \times o_i(\tau)}$$

$$\pi_4 = g^{q(\tau)}$$

$$\pi_1 = g^{\sum c_i \times l_i(\tau) + \delta_1 V(\tau)}$$

$$\pi_2 = g^{\sum c_i \times r_i(\tau) + \delta_2 V(\tau)}$$

$$\pi_3 = g^{\sum c_i \times o_i(\tau) + \delta_3 V(\tau)}$$

$$\pi_4 = g^{q(\tau)}$$

Vで割り切れるランダム値を足すことで検証アルゴリズムはそのままでOK

m: mul gateの数

まとめ

- Groth16はQAPとLinear PCPによって構成されるSNARK
- 回路→トレース→セレクター多項式→マスター多項式→Linear PCPで証明
- Groth16は1回のペアリングで検証できる

参考資料

- https://rdi.berkeley.edu/zk-learning/assets/lecture9.pdf

演習問題

1) QAPのトレースがなぜ加算ゲートの出力を記録しなくてもいいのか、理由を説明してください。（ヒント: Linear PCP）
2) 講義で紹介された算術回路とセレクター多項式をもとにマスター多項式p(x)と商多項式q(x)を一つ考えてください。
3) Linear PCPベースのSNARKとGroth16がどのような安全性仮定に基づいているか説明してください。(ヒント: Generic Group Model, KoE Assumption)

Thank you!