SNARK Pack Design

1. Groth16 Proof

$\pi = (A, B, C)$, $A, C \in G_1$, $B \in G_2$

pairing check:

$$e(A, B) = Y \cdot e(C, D)$$

2. Agg Groth16 Proofs:

$\pi_i = (A_i, B_i, C_i)$

$$\underbrace{\prod_{i=0}^{k-1} e(A_i, B_i)^{r_i}}_{Z_{AB}} = \underbrace{\prod_{i=0}^{k-1} Y_i^{r_i} \cdot e(\prod_{i=0}^{k-1} C_i^{r_i}, D)}_{Z_C}$$

In addition to final pairing check, the prover needs to show two inner product relations:

- TIPP: $CM(A) \in G_1$, $CM(B) \in G_2$, $Z_{AB} = \prod_{i=0}^{k-1} e(A_i, B_i)$
- MIPP: $CM(C) \in G_1$, $r \in Z_p$, $Z_C = \prod_{i=0}^{k-1} C_i^{r_i}$

??

3. Inner Product Relations

$\boxed{\text{Def 1. Inner Product Map}}$

$\circledast : M_1 \times M_2 \to M_3$ is an Inner Product Map i.e.: $a, b \in M_1$, $c, d \in M_2$.

$$(a+b) \circledast (c+d) = a \circledast c + a \circledast d + b \circledast c + b \circledast d$$

$$\langle \vec{a}, \vec{b} \rangle = \sum_{i=0}^{k-1} a_i \circledast b_i$$

Example: in TIPP: $\circledast : G_1 \times G_2 \to G_T$

MIPP: $\circledast : G \times F \to G$

Def 2: Doubly Homomorphic Commitment Scheme

$(K, +)$, $(M, +)$. $(\mathrm{Image}(CM), +)$ define abelian groups.

s.t.

1. $CM(ck; M) + CM(ck; M') = CM(ck; M + M')$

2. $CM(ck; M) + CM(ck'; M) = CM(ck + ck', M)$

Collary: $CM(x \cdot ck, M) = CM(ck, x \cdot M)$

Def 3. Inner Product Commitment

Let (Setup, CM) be a doubly homomorphic commitment with

$$M = M_1^k \times M_2^k \times M_3 \qquad \text{for } \forall\ k \in [2^j]_{j \in N}$$
$$K = K_1^k \times K_2^k \times K_3$$

(Setup, CM, $\circledast$) is an inner product commitment iff

an efficient function Collapse exist:

$$\mathrm{Collapse}\left(CM\left(\begin{matrix} ck_1 \| ck_1' \\ ck_2 \| ck_2' \\ ck_3 \end{matrix} \middle| \begin{matrix} M_1 \| M_1 \\ M_2 \| M_2 \\ M_3 \end{matrix}\right)\right) = CM\left(\begin{matrix} ck_1 + ck_1' \\ ck_2 + ck_2' \\ ck_3 \end{matrix} \middle| \begin{matrix} M_1 \\ M_2 \\ M_3 \end{matrix}\right)$$

4. Inner Product Argument (GIPA)

goal: ~~prove~~ $C = \langle \vec{a}, \vec{b} \rangle$

warm up: prove $a_1 \circledast b_1 + a_2 \circledast b_2 = C$,

reduce the instance to a single $\circledast$

Prover		Verifier
$l = a_1 \circledast b_2$ $r = a_2 \circledast b_1$	$\longrightarrow$	l, r
	$\xleftarrow{x \leftarrow \$}$	

$a' = x \cdot a_1 + a_2$

$b' = x^{-1} \cdot b_1 + b_2$

now the instance become: $l, r,\ a' \circledast b = x \cdot l + C + x^{-1} \cdot r$

GIPA generalize the warm-up instance to $\vec{a_1}, \vec{a_2}, \vec{b_1}, \vec{b_2}$

prove $(ck = (ck_1, ck_2, ck_3); (\vec{a}, \vec{b}))$ Verify(ck, C)

if $m = 1$

$a \in M_1,\ b \in M_2,\ CM(ck; (a, b, a \circledast b)) == C$

Else $m \geq 2$

$m' = m/2$

$z_1 = \langle \vec{a}_{[m':]}, \vec{b}[:m'] \rangle$

$$z_R = \langle \vec{a}_{[:m']}, \vec{b}[m':] \rangle$$

$$C_L = CM(ck_1, ck_2, ck_3;\ a_{[m':]} \| 0,\ 0 \| b[:m'],\ z_L)$$

$$C_R = CM(ck_1, ck_2, ck_3;\ 0 \| a[:m'],\ b[m':] \| 0,\ z_R)$$

$$\xrightarrow{C_L,\ C_R}$$

$$\xleftarrow{x} \qquad \underline{x \xleftarrow{\$} F_p}$$

$$\vec{a}' = \vec{a}_{[:m']} + x \cdot \vec{a}_{[m':]}$$

$$\vec{b}' = \vec{b}[:m'] + x^{-1} \cdot \vec{b}[m':]$$

$$ck_1' = ck_{1,[:m']} + x^{-1} \cdot ck_{1,[m':]} \qquad \underline{ck_1' = ck_{1,[:m']} + x^{-1} \cdot ck_{1,[}}$$

$$ck_2' = ck_{2,[:m']} + x \cdot ck_{2,[m':]} \qquad \underline{ck_2' = ck_{2,[:m']} + x \cdot ck_{2,[}}$$

$$\underline{C' = \text{Collapse}(x \cdot C_L + C + x^{-1} \cdot C_R)}$$

Recurse on $(ck_1', ck_2', ck_3); (\vec{a}', \vec{b}'))$ <u>Recurse on</u> $\underline{((ck_1', ck_2', ck_3), C')}$

How dose Collapse Work?

$$x^{-1} \cdot C_R + C + x \cdot C_L$$

$$= x^{-1} \left(\begin{matrix} ck_1[:m'] \| ck_1[m':], \\ ck_2[:m'] \| ck_2[m':], \end{matrix} \middle| \begin{matrix} 0 \| a[:m'] \\ b[m':] \| 0, \end{matrix} \right)$$

$$
\quad ck_3 \qquad\qquad \Big| \qquad \langle a[:m'], b[m':] \rangle \Big)
$$

$$
+ \left(\begin{array}{c|c}
ck_1[:m'] \,\|\, ck_1[m':], & a, \\
ck_2[:m'] \,\|\, ck_2[m':], & b, \\
ck_3 & a \circledast b
\end{array} \right)
$$

$$
+ \; x \left(\begin{array}{c|c}
ck_1[:m'] \,\|\, ck_1[m':], & a[m':] \,\|\, 0, \\
ck_2[:m'] \,\|\, ck_2[m':], & 0 \,\|\, b[:m'], \\
ck_3 & \langle a[m':], b[:m'] \rangle
\end{array} \right)
$$