PLONK

- ZK PROOF
- PLONK - general-purpose ZKP ("Permutations over Lagrange - bases for Oecumenical Noninteractive arguments of Knowledge", Ariel Gabizon, Zac Williamson, Oana Ciobotaru)

PLONK

- ZK PROOF
- PLONK - general-purpose ZKP ("Permutations over Lagrange - bases for Oecumenical Noninteractive arguments of Knowledge", Ariel Gabizon, Zac Williamson, Oana Ciobotaru)
- PLONK uses KATE PCS (trusted setup and elliptic curve pairing).

On PLONK – Polynomials

Let $f \in \mathbb{F}_p[x]$. If $f(x) = 0$, for $\forall x \in H$, where $H = \{h_1, \ldots, h_n\}$, than

$$f(x) = (x - h_1)(x - h_2) \cdot \ldots \cdot (x - h_n) \cdot t(x) = Z_H(x) \cdot t(x). \quad (1)$$

★ Schwartz - Zippel lemma ★

The main idea (Level 1)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$): Andrija:

$z \xleftarrow{R} \mathbb{F}_p$

$< - - - - z - - - -$

The main idea (Level 1)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$): Andrija:

$z \xleftarrow{R} \mathbb{F}_p$

$< - - - - z - - - -$

$f(z),\ t(z)$

$- - f(z),\ t(z) - - >$

The main idea (Level 1)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$): Andrija:

$z \xleftarrow{R} \mathbb{F}_p$

$< - - - - z - - - -$

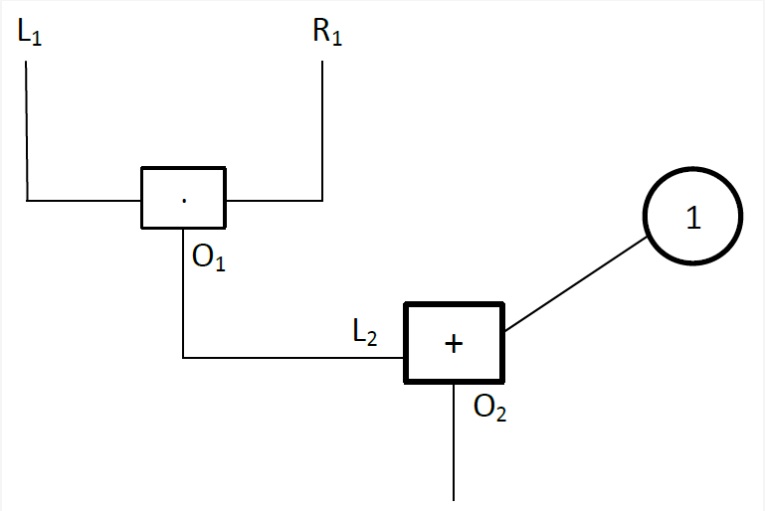
$f(z),\ t(z)$

$- - f(z),\ t(z) - - >$

$f(z) == Z_H(z) \cdot t(z)$

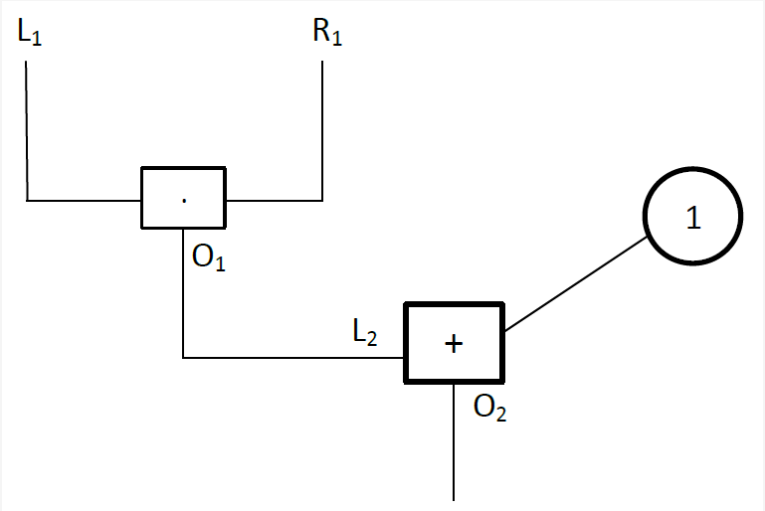
From arithmetic circuits to constraint system

Example. $a^2 = b - 1$



From arithmetic circuits to constraint system

Example. $a^2 = b - 1$



System constraints:

Gate constraints:

(1) $L_1 \cdot R_1 - O_1 = 0$

(2) $L_2 + 1 - O_2 = 0$

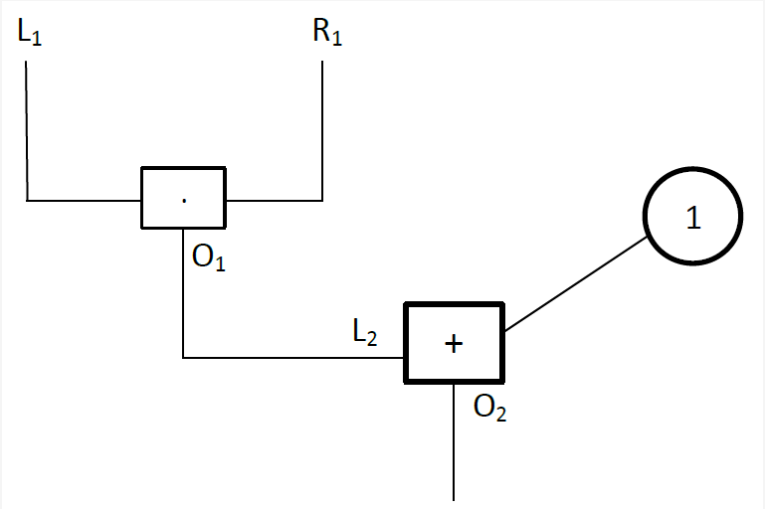
Copy constraints:

$L_1 = R_1$

$O_1 = L_2$

From arithmetic circuits to constraint system

Example. $a^2 = b - 1$



System constraints:

Gate constraints:

(1) $L_1 \cdot R_1 - O_1 = 0$

(2) $L_2 + 1 - O_2 = 0$

Copy constraints:

$L_1 = R_1$

$O_1 = L_2$

$$L_i \cdot q_{L_i} + R_i \cdot q_{R_i} + O_i \cdot q_{O_i} + q_{C_i} + L_i \cdot R_i \cdot q_{M_i} = 0. \qquad (2)$$

From constraint system to polynomials

Define $L(x), R(x), O(x)$:

$$L(1) = L_1,\ L(2) = L_2,\ R(1) = R_1,\ R(2) = R_2,\ O(1) = O_1,\ O(2) = O_2.$$

$$f(x) = L(x)\cdot q_L(x) + R(x)\cdot q_R(x) + O(x)\cdot q_O(x) + q_C(x) + L(x)\cdot R(x)\cdot q_M(x).$$

The main idea (Level 2)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$): Andrija:

$z \xleftarrow{R} \mathbb{F}_p$

$< - - - - z - - - - - - -$

The main idea (Level 2)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$): Andrija:

$z \xleftarrow{R} \mathbb{F}_p$

$< - - - - z - - - - - - -$

$L(z),\ R(z),\ O(z),\ t(z)$

$-L(z), R(z), O(z), t(z) - >$

The main idea (Level 2)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$): Andrija:

$z \xleftarrow{R} \mathbb{F}_p$

$< - - - - z - - - - - - -$

$L(z),\ R(z),\ O(z),\ t(z)$

$-L(z), R(z), O(z), t(z) - >$

$f(z) == Z_H(z) \cdot t(z)$

KATE (KGZ) polynomial commitment sheme (Level 1)

$com(f)$ – hides polynomial

SETUP

1. $s \xleftarrow{R} \mathbb{F}_p$
2. $\{G, [s]_1, [s^2]_1, \ldots, [s^k]_1\}$ – CRS (common reference string)

KATE (KGZ) polynomial commitment sheme (Level 1)

$com(f)$ – hides polynomial

SETUP

1. $s \xleftarrow{R} \mathbb{F}_p$
2. $\{G, [s]_1, [s^2]_1, \ldots, [s^k]_1\}$ – CRS (common reference string)

COMMIT

$$com(f) = f(s) \cdot G$$

KATE (KGZ) polynomial commitment sheme (Level 1)

$com(f)$ – hides polynomial

SETUP

1. $s \xleftarrow{R} \mathbb{F}_p$
2. $\{G, [s]_1, [s^2]_1, \ldots, [s^k]_1\}$ – CRS (common reference string)

COMMIT

$$com(f) = f(s) \cdot G$$

EVALUATION PROOF

$z - - > f(z)$, π (proof that is f(z))
$f(x) - f(z) = (x - z) \cdot h(x)$

Andrija: $com(f) - com(f(z)) = com(s - z) \cdot com(h(s))$

The main idea (Level 3)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$):

Andrija:

$com(L)$, $com(R)$
$com(O)$, $com(t)$

$$-com(L), com(R), com(O), com(t) - >$$

The main idea (Level 3)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$): Andrija:

$com(L)$, $com(R)$
$com(O)$, $com(t)$

$$-com(L), com(R), com(O), com(t) - >$$

$$z \xleftarrow{R} \mathbb{F}_p$$

$$< - - - - z - - - - - -$$

The main idea (Level 3)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$): Andrija:

$com(L)$, $com(R)$
$com(O)$, $com(t)$

$$-com(L), com(R), com(O), com(t) - >$$

$$z \xleftarrow{R} \mathbb{F}_p$$

$$< - - - - z - - - - - -$$

$com(L(z)), com(R(z))$
$com(O(z)), com(t(z))$

$$-com(L(z)), com(R(z)), com(O(z)), com(t(z)) - >$$

$$- - - - com(h) - - - - >$$

The main idea (Level 3)

Public: $H = \{h_1, \ldots, h_n\}$

Marija (knows $f(x)$): Andrija:

$com(L)$, $com(R)$
$com(O)$, $com(t)$

$$-com(L), com(R), com(O), com(t) - >$$

$$z \xleftarrow{R} \mathbb{F}_p$$

$$< - - - - z - - - - - -$$

$com(L(z)), com(R(z))$
$com(O(z)), com(t(z))$

$$-com(L(z)), com(R(z)), com(O(z)), com(t(z)) - >$$

$$- - - - com(h) - - - - >$$

♡?

KATE (KGZ) polynomial commitment sheme (Level 1)

Note that:

- $com(A) = com(B) <=> A = B$

KATE (KGZ) polynomial commitment sheme (Level 1)

Note that:

- $com(A) = com(B) <=> A = B$
- $com(A) + com(B) = com(A + B)$

KATE (KGZ) polynomial commitment sheme (Level 1)

Note that:

- $com(A) = com(B) <=> A = B$
- $com(A) + com(B) = com(A + B)$
- $com(f(s) - f(z)) = com(f) - com(f(z)) = com((s - z) \cdot h(s))$

KATE (KGZ) polynomial commitment sheme (Level 1)

Note that:

- $com(A) = com(B) <=> A = B$
- $com(A) + com(B) = com(A + B)$
- $com(f(s) - f(z)) = com(f) - com(f(z)) = com((s - z) \cdot h(s))$

$$com((s - z) \cdot h(s)) = com(s - z) \cdot com(h(s))?!$$

KATE (KGZ) polynomial commitment sheme (Level 1)

Note that:

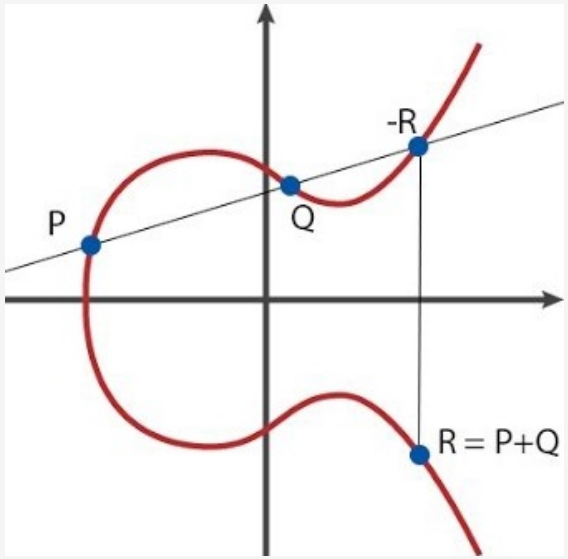
- $com(A) = com(B) <=> A = B$
- $com(A) + com(B) = com(A + B)$
- $com(f(s) - f(z)) = com(f) - com(f(z)) = com((s - z) \cdot h(s))$

$$com((s - z) \cdot h(s)) = com(s - z) \cdot com(h(s))?!$$

Elliptic curve pairing!!!

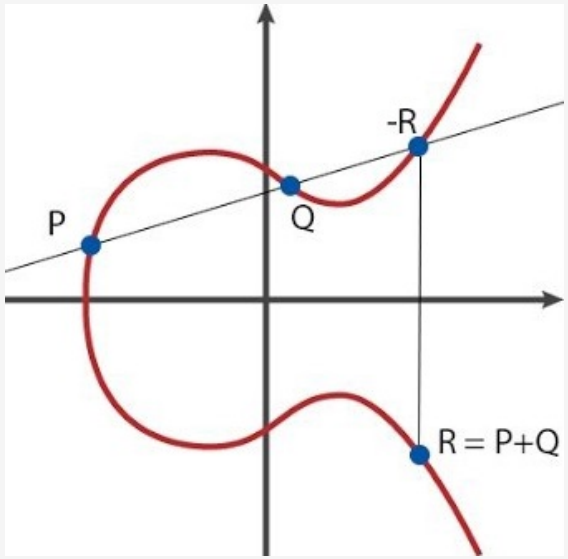
A little bit about elliptic curves and pairings

$$y^2 = x^3 + b$$



A little bit about elliptic curves and pairings

$$y^2 = x^3 + b$$



G_1, G_2 – subgroup of elliptic curve, G generator of G_1, H generator of G_2

$e : G_1 \times G_2 \to G_T$:

1) $e(P + Q, R) = e(P, R) \cdot e(Q, R)$
2) $e(P, Q + R) = e(P, Q) \cdot e(P, R)$
3) $e([a]_1, [b]_2) = e(G, H)^{ab}$

KATE (KGZ) polynomial commitment sheme (Level 2)

SETUP

1. $s \xleftarrow{R} \mathbb{F}_p$
2. $[s^i]_1, [s]_2$, $i \in \{0, 1, \ldots, n\}$ – CRS (common reference string)

KATE (KGZ) polynomial commitment sheme (Level 2)

SETUP

1. $s \xleftarrow{R} \mathbb{F}_p$
2. $[s^i]_1, [s]_2$, $i \in \{0, 1, \ldots, n\}$ – CRS (common reference string)

COMMIT

$com(f) = [f(s)]_1$

KATE (KGZ) polynomial commitment sheme (Level 2)

SETUP

1. $s \xleftarrow{R} \mathbb{F}_p$
2. $[s^i]_1, [s]_2$, $i \in \{0, 1, \ldots, n\}$ – CRS (common reference string)

COMMIT

$$com(f) = [f(s)]_1$$

EVALUATION PROOF

$$\pi = [h(s)]_1$$

KATE (KGZ) polynomial commitment sheme (Level 2)

SETUP

1. $s \xleftarrow{R} \mathbb{F}_p$
2. $[s^i]_1, [s]_2$, $i \in \{0, 1, \ldots, n\}$ – CRS (common reference string)

COMMIT

$$com(f) = [f(s)]_1$$

EVALUATION PROOF

$$\pi = [h(s)]_1$$

Finally, Andrija can check:

$$\heartsuit: \; e(\pi, [s - z]_2) == e(com(f) - [f(z)]_1, H)$$