Groth16

Saravanan Vijayakumaran

Department of Electrical Engineering
Indian Institute of Technology Bombay

December 19, 2023

Groth16

- In 2016, Jens Groth published a paper titled
  On the Size of Pairing-based Non-interactive Arguments
- He described a pairing-based zkSNARK which was more efficient than previous proposals
  - Proof consisted of 3 elliptic curve group elements
  - Verification involved checking a single pairing product equation
- Real-world usage
  - Tornado Cash
  - Filecoin
  - Dark Forest
- To use Groth16
  - Statement has to expressed as a quadratic arithmetic program
  - A trusted setup has to be performed to generate a structured reference string (SRS)

Group Theory Recap

Groups

Definition

A set G with a binary operation $\star$ defined on it is called a group if

- the operation $\star$ is closed,
- the operation $\star$ is associative,
- there exists an identity element $e \in G$ such that for any $a \in G$

$$a \star e = e \star a = a,$$

- for every $a \in G$, there exists an element $b \in G$ such that

$$a \star b = b \star a = e.$$

Example

- Modulo n addition on $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

Definition

A group G is said to be abelian if $a \star b = b \star a$ for all $a, b \in G$

Cyclic Groups

Definition

A finite group is a group with a finite number of elements. The order of a finite group G is its cardinality.

Definition

A cyclic group is a finite group G such that each element in G appears in the sequence

$$\{g, g \star g, g \star g \star g, \ldots\}$$

for some particular element $g \in G$, which is called a generator of G. We write $G = \langle g \rangle$

Example

- For an integer $n \geq 1$, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$
  - Operation is addition modulo n
  - $\mathbb{Z}_n$ is cyclic with generator 1

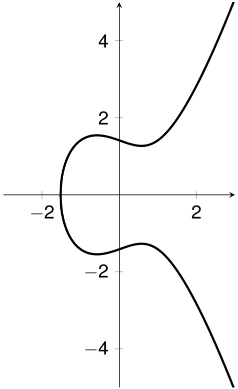
Elliptic Curves Over Real Numbers

Elliptic Curves over Reals

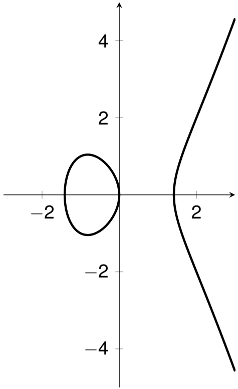
The set E of real solutions (x, y) of

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

along with a "point of infinity" $\mathcal{O}$. Here $4a^3 + 27b^2 \neq 0$.

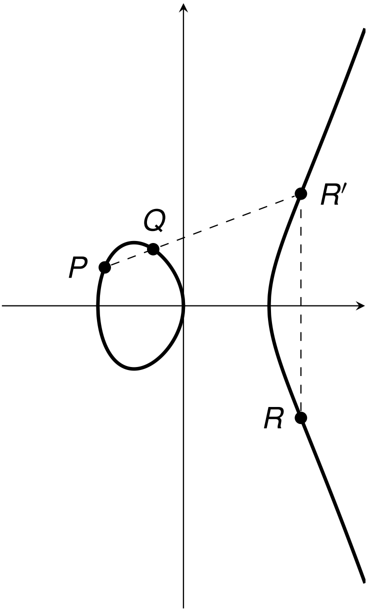


$y^2 = x^3 - x + 2$



$y^2 = x^3 - 2x$

Point Addition (1/3)



$$P = (x_1, y_1), Q = (x_2, y_2)$$

$$x_1 \neq x_2$$

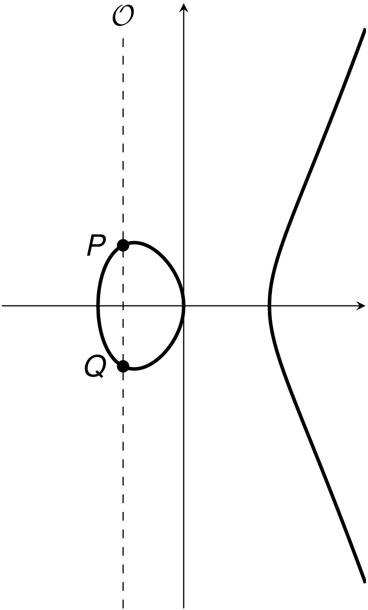
$$P + Q = R$$

$$R = (x_3, y_3)$$

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

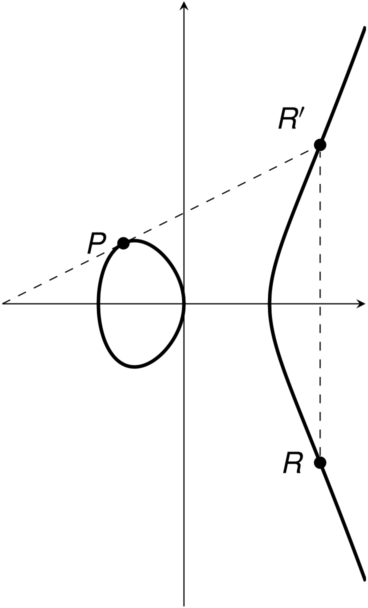
$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

Point Addition (2/3)



$$P = (x_1, y_1), Q = (x_2, y_2)$$
$$x_1 = x_2, y_1 = -y_2$$
$$P + Q = \mathcal{O}$$

Point Addition (3/3)



$$P = (x_1, y_1), Q = (x_2, y_2)$$
$$x_1 = x_2, y_1 = y_2 \neq 0$$
$$P + Q = R$$

$$R = (x_3, y_3)$$
$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$
$$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

Elliptic Curves Over Finite Fields

Fields

Definition

A set F together with two binary operations $+$ and $*$ is a field if

- F is an abelian group under $+$ whose identity is called 0
- $F^* = F \setminus \{0\}$ is an abelian group under $*$ whose identity is called 1
- For any $a, b, c \in F$

$$a * (b + c) = a * b + a * c$$

Definition

A finite field is a field with a finite cardinality.

Prime Fields

- $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ where p is prime
- $+$ and $*$ defined on $\mathbb{F}_p$ as

$$x + y = x + y \bmod p,$$
$$x * y = xy \bmod p.$$

- $\mathbb{F}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- In fields, division is multiplication by multiplicative inverse

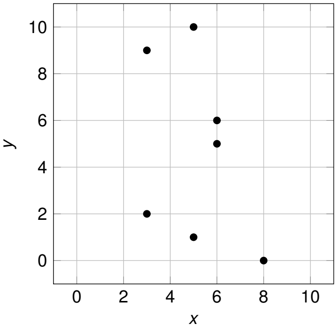
$$\frac{x}{y} = x * y^{-1}$$

Elliptic Curves over Finite Fields

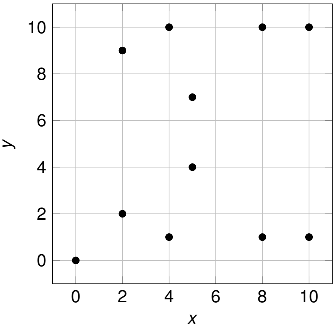
For $\text{char}(F) \neq 2, 3$, the set E of solutions (x, y) in F^2 of

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

along with a "point of infinity" $\mathcal{O}$. Here $4a^3 + 27b^2 \neq 0$.



$y^2 = x^3 + 10x + 2$ over $\mathbb{F}_{11}$



$y^2 = x^3 + 9x$ over $\mathbb{F}_{11}$

Point Addition for Finite Field Curves

- Point addition formulas derived for reals are used
- Example: $y^2 = x^3 + 10x + 2$ over $\mathbb{F}_{11}$

$+$	$\mathcal{O}$	$(3,2)$	$(3,9)$	$(5,1)$	$(5,10)$	$(6,5)$	$(6,6)$	$(8,0)$
$\mathcal{O}$	$\mathcal{O}$	$(3,2)$	$(3,9)$	$(5,1)$	$(5,10)$	$(6,5)$	$(6,6)$	$(8,0)$
$(3,2)$	$(3,2)$	$(6,6)$	$\mathcal{O}$	$(6,5)$	$(8,0)$	$(3,9)$	$(5,10)$	$(5,1)$
$(3,9)$	$(3,9)$	$\mathcal{O}$	$(6,5)$	$(8,0)$	$(6,6)$	$(5,1)$	$(3,2)$	$(5,10)$
$(5,1)$	$(5,1)$	$(6,5)$	$(8,0)$	$(6,6)$	$\mathcal{O}$	$(5,10)$	$(3,9)$	$(3,2)$
$(5,10)$	$(5,10)$	$(8,0)$	$(6,6)$	$\mathcal{O}$	$(6,5)$	$(3,2)$	$(5,1)$	$(3,9)$
$(6,5)$	$(6,5)$	$(3,9)$	$(5,1)$	$(5,10)$	$(3,2)$	$(8,0)$	$\mathcal{O}$	$(6,6)$
$(6,6)$	$(6,6)$	$(5,10)$	$(3,2)$	$(3,9)$	$(5,1)$	$\mathcal{O}$	$(8,0)$	$(6,5)$
$(8,0)$	$(8,0)$	$(5,1)$	$(5,10)$	$(3,2)$	$(3,9)$	$(6,6)$	$(6,5)$	$\mathcal{O}$

- The set $E \cup \mathcal{O}$ is closed under addition
- In fact, its a group

Bilinear Pairings

- Let G_1, G_2 and G_T be three cyclic groups of prime order p
- G_1, G_2 are elliptic curve groups and G_T is subgroup of $\mathbb{F}^*_{r^n}$ where r is a prime
- Let $G_1 = \langle g \rangle$ and $G_2 = \langle h \rangle$
- A **pairing** is a efficient map $e : G_1 \times G_2 \mapsto G_T$ satisfying
  1. **Bilinearity**: $\forall \alpha, \beta \in \mathbb{Z}_p$, we have $e(g^\alpha, h^\beta) = e(g, h)^{\alpha\beta}$
  2. **Non-degeneracy**: $e(g, h)$ is not the identity in G_T
- Finding discrete logs is assumed to be difficult in all 3 groups
- Pairings enable multiplication of secrets

Non-interactive Linear Proofs for QAPs

Quadratic Arithmetic Programs

- Recall that a quadratic arithmetic program is given by

$$R = \left(\mathbb{F}, l, \{u_i(X), v_i(X), w_i(X)\}_{i=0}^{m}, t(X)\right)$$

  where

  - $\mathbb{F}$ is a finite field
  - l is the number of variables expressing the statement, $1 \leq l \leq m$
  - $t(X) = \prod_{q=1}^{n}(X - r_q)$ for $r_1, r_2, \ldots, r_n$ in $\mathbb{F}$

- Such a QAP defines a language L with $a_0 = 1$ where

  - L is the set of $\phi = (a_1, a_2, \ldots, a_l) \in \mathbb{F}^l$ such that
  - there exists a $\psi = (a_{l+1}, a_{l+2}, \ldots, a_m) \in \mathbb{F}^{m-l}$ satisfying

$$\left(\sum_{i=0}^{m} a_i u_i(X)\right)\left(\sum_{i=0}^{m} a_i v_i(X)\right) = \left(\sum_{i=0}^{m} a_i w_i(X)\right) \bmod t(X)$$

- The last equation can be rewritten as

$$\left(\sum_{i=0}^{m} a_i u_i(X)\right)\left(\sum_{i=0}^{m} a_i v_i(X)\right) = \left(\sum_{i=0}^{m} a_i w_i(X)\right) + h(X)t(X)$$

  for some degree $n - 2$ quotient polynomial $h(X)$

Non-interactive Linear Proofs for QAPs

- $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \leftarrow \text{Setup}(R)$
  Pick $\alpha, \beta, \gamma, \delta, x \leftarrow \mathbb{F}^*$. Set

$$\boldsymbol{\tau} = (\alpha, \beta, \gamma, \delta, x)$$

$$\boldsymbol{\sigma} = \left(\alpha, \beta, \gamma, \delta, \left\{x^i\right\}_{i=0}^{n-1}, \left\{\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}\right\}_{i=0}^{l}, \left\{\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta}\right\}_{i=l+1}^{m}, \left\{\frac{x^i t(x)}{\delta}\right\}_{i=0}^{n-2}\right)$$

- $\boldsymbol{\pi} \leftarrow \text{Prove}(R, \boldsymbol{\sigma}, a_1, \ldots, a_M)$
  Pick $r, s \leftarrow \mathbb{F}$ and compute a $3 \times (m + 2n + 4)$ matrix Π such that $\boldsymbol{\pi} = \Pi\boldsymbol{\sigma} = (A, B, C)$ where

$$A = \alpha + \sum_{i=0}^{m} a_i u_i(x) + r\delta, \qquad B = \beta + \sum_{i=0}^{m} a_i v_i(x) + s\delta$$

$$C = \frac{\sum_{i=l+1}^{m} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right) + h(x)t(x)}{\delta} + As + Br - rs\delta$$

- $0/1 \leftarrow \text{Verify}(R, \boldsymbol{\sigma}, a_1, \ldots, a_l, \boldsymbol{\pi})$: Check if

$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

Schwartz-Zippel Lemma

Lemma

Let $\mathbb{F}$ be a finite field. For any nonzero polynomial $f \in \mathbb{F}[x]$ of degree d

$$\Pr\left[f(s) = 0\right] \leq \frac{d}{|\mathbb{F}|}$$

when s is chosen uniformly from $\mathbb{F}$.

Corollary

For two distinct polynomials $f, g \in \mathbb{F}[x]$

$$\Pr\left[f(s) = g(s)\right] \leq \frac{d}{|\mathbb{F}|}$$

when s is chosen uniformly from $\mathbb{F}$.

Soundness of the NILP

- Suppose the prover generated (A, B, C) as $\Pi\boldsymbol{\sigma}$ which satisfies

$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

- We want to show that the prover knows a QAP witness $(a_{l+1}, \ldots, a_m)$ for the statement $(a_1, \ldots, a_l)$
- Recall that

$$\boldsymbol{\sigma} = \left(\alpha, \beta, \gamma, \delta, \left\{x^i\right\}_{i=0}^{n-1}, \left\{\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}\right\}_{i=0}^{l}, \right.$$
$$\left. \left\{\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta}\right\}_{i=l+1}^{m}, \left\{\frac{x^i t(x)}{\delta}\right\}_{i=0}^{n-2}\right)$$

- So A is of the form

$$A = A_\alpha \alpha + A_\beta \beta + A_\gamma \gamma + A_\delta \delta + A(x) + \sum_{i=0}^{l} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$
$$\sum_{i=l+1}^{m} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + A_h(x) \frac{t(x)}{\delta}$$

- B and C have similar forms

Soundness of the NILP

- We have

$$A = A_\alpha \alpha + A_\beta \beta + A_\gamma \gamma + A_\delta \delta + A(x) + \sum_{i=0}^{l} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$\sum_{i=l+1}^{m} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + A_h(x) \frac{t(x)}{\delta}$$

$$B = B_\alpha \alpha + B_\beta \beta + B_\gamma \gamma + B_\delta \delta + B(x) + \sum_{i=0}^{l} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$\sum_{i=l+1}^{m} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + B_h(x) \frac{t(x)}{\delta}$$

- By the Schwartz-Zippel lemma, the coefficients on either side of below equation should match

$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

- Since there is no α^2 on the right, $A_\alpha B_\alpha = 0$
  - WLOG, let $B_\alpha = 0$

Soundness of the NILP

- We have

$$A = A_\alpha \alpha + A_\beta \beta + A_\gamma \gamma + A_\delta \delta + \dots$$
$$B = B_\beta \beta + B_\gamma \gamma + B_\delta \delta + \dots$$
$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

- Since the coefficient of $\alpha\beta$ is 1 on the right, $A_\alpha B_\beta = 1$
- Since AB can be written as $(AA_\alpha) \cdot (BB_\beta)$, assume $A_\alpha = B_\beta = 1$
- Since there is no β^2 term on the right of AB, we get $A_\beta B_\beta = A_\beta = 0$
- A and B can be simplified to

$$A = \alpha + A_\gamma \gamma + A_\delta \delta + A(x) + \sum_{i=0}^{l} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$
$$\sum_{i=l+1}^{m} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + A_h(x) \frac{t(x)}{\delta}$$

$$B = \beta + B_\gamma \gamma + B_\delta \delta + B(x) + \sum_{i=0}^{l} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$
$$\sum_{i=l+1}^{m} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + B_h(x) \frac{t(x)}{\delta}$$

Soundness of the NILP

- We have

$$A = \alpha + A_\gamma \gamma + A_\delta \delta + A(x) + \sum_{i=0}^{l} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$\sum_{i=l+1}^{m} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + A_h(x) \frac{t(x)}{\delta}$$

$$B = \beta + B_\gamma \gamma + B_\delta \delta + B(x) + \sum_{i=0}^{l} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$\sum_{i=l+1}^{m} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + B_h(x) \frac{t(x)}{\delta}$$

$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

- Since there is no term involving $\frac{1}{\delta^2}$ on the right of AB, we have

$$\left(\sum_{i=l+1}^{m} A_i(\beta u_i(x) + \alpha v_i(x) + w_i(x)) + A_h(x)t(x)\right)$$

$$\cdot \left(\sum_{i=l+1}^{m} B_i(\beta u_i(x) + \alpha v_i(x) + w_i(x)) + B_h(x)t(x)\right) = 0$$

Soundness of the NILP

- We have

$$A = \alpha + A_\gamma \gamma + A_\delta \delta + A(x) + \sum_{i=0}^{l} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$B = \beta + B_\gamma \gamma + B_\delta \delta + B(x) + \sum_{i=0}^{l} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$\sum_{i=l+1}^{m} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + B_h(x) \frac{t(x)}{\delta}$$

$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

- Since there is no term involving $\frac{\alpha}{\delta}$ on the right of AB, we have

$$\sum_{i=l+1}^{m} B_i(\beta u_i(x) + \alpha v_i(x) + w_i(x)) + B_h(x) t(x) = 0$$

Soundness of the NILP

- We have

$$A = \alpha + A_\gamma \gamma + A_\delta \delta + A(x) + \sum_{i=0}^{l} A_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$B = \beta + B_\gamma \gamma + B_\delta \delta + B(x) + \sum_{i=0}^{l} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

- Since there is no term involving $\frac{1}{\gamma^2}$ on the right of AB, we have

$$\left(\sum_{i=0}^{l} A_i(\beta u_i(x) + \alpha v_i(x) + w_i(x))\right) \cdot \left(\sum_{i=0}^{l} B_i(\beta u_i(x) + \alpha v_i(x) + w_i(x))\right) = 0$$

- WLOG, assume that $\sum_{i=0}^{l} A_i(\beta u_i(x) + \alpha v_i(x) + w_i(x)) = 0$

Soundness of the NILP

- We have

$$A = \alpha + A_\gamma \gamma + A_\delta \delta + A(x)$$

$$B = \beta + B_\gamma \gamma + B_\delta \delta + B(x) + \sum_{i=0}^{l} B_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

- Since there is no term involving $\frac{\alpha}{\gamma}$ on the right of AB, we have

$$\sum_{i=0}^{l} B_i(\beta u_i(x) + \alpha v_i(x) + w_i(x)) = 0$$

- Since there is no term involving $\beta\gamma$ or $\alpha\gamma$ on the right of AB, we have $A_\gamma = 0$ and $B_\gamma = 0$
- A and B can be simplified to

$$A = \alpha + A_\delta \delta + A(x)$$

$$B = \beta + B_\delta \delta + B(x)$$

Soundness of the NILP

- We have

$$A = \alpha + A_\delta \delta + A(x)$$
$$B = \beta + B_\delta \delta + B(x)$$
$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

- Recall that

$$C = C_\alpha \alpha + C_\beta \beta + C_\gamma \gamma + C_\delta \delta + C(x) + \sum_{i=0}^{l} C_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$
$$\sum_{i=l+1}^{m} C_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + C_h(x) \frac{t(x)}{\delta}$$

- Equating the terms involving α and β in the verification equation, we get

$$\alpha B(x) = \sum_{i=0}^{l} a_i \alpha v_i(x) + \sum_{i=l+1}^{m} C_i \alpha v_i(x)$$
$$\beta A(x) = \sum_{i=0}^{l} a_i \beta u_i(x) + \sum_{i=l+1}^{m} C_i \beta u_i(x)$$

Soundness of the NILP

- We have

$$B(x) = \sum_{i=0}^{l} a_i v_i(x) + \sum_{i=l+1}^{m} C_i v_i(x)$$

$$A(x) = \sum_{i=0}^{l} a_i u_i(x) + \sum_{i=l+1}^{m} C_i u_i(x)$$

- Defining $a_i = C_i$ for $i = l + 1, \ldots, m$ we have

$$A(x) = \sum_{i=0}^{m} a_i u_i(x), \qquad B(x) = \sum_{i=0}^{m} a_i v_i(x)$$

Soundness of the NILP

- We have

$$A = \alpha + A_\delta \delta + \sum_{i=0}^{m} a_i u_i(x)$$

$$B = \beta + B_\delta \delta + \sum_{i=0}^{m} a_i v_i(x)$$

$$A \cdot B = \alpha \cdot \beta + \frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma} \cdot \gamma + C \cdot \delta$$

- Recall that

$$C = C_\alpha \alpha + C_\beta \beta + C_\gamma \gamma + C_\delta \delta + C(x) + \sum_{i=0}^{l} C_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}$$

$$\sum_{i=l+1}^{m} C_i \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} + C_h(x) \frac{t(x)}{\delta}$$

- Equating the terms in the verification equation involving only powers of x in

$$\left(\sum_{i=0}^{m} a_i u_i(x)\right)\left(\sum_{i=0}^{m} a_i v_i(x)\right) = \sum_{i=0}^{m} a_i w_i(x) + C_h(x) t(x)$$

- This shows that $(a_{l+1}, \ldots, a_m)$ is a witness for the statement $(a_1, \ldots, a_l)$

Enforcing a Linear Prover

- Suppose we have an elliptic curve pairing $e : G_1 \times G_2 \to G_T$
- Let $G_1 = \langle g \rangle$ and $G_2 = \langle h \rangle$ both having order p
- For $\alpha \in \mathbb{Z}_p$, let $[\alpha]_1 = g^\alpha$ and $[\alpha]_2 = h^\alpha$
- $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \leftarrow \text{Setup}(R)$
  Pick $\alpha, \beta, \gamma, \delta, x \leftarrow \mathbb{Z}_p^*$. Set

$$\boldsymbol{\tau} = (\alpha, \beta, \gamma, \delta, x)$$
$$\boldsymbol{\sigma} = ([\boldsymbol{\sigma}_1]_1, [\boldsymbol{\sigma}_2]_2)$$

where

$$\boldsymbol{\sigma}_1 = \left(\alpha, \beta, \gamma, \delta, \left\{ x^i \right\}_{i=0}^{n-1}, \left\{ \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma} \right\}_{i=0}^{l}, \left\{ \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta} \right\}_{i=l+1}^{m}, \left\{ \frac{x^i t(x)}{\delta} \right\}_{i=0}^{n-2} \right)$$

$$\boldsymbol{\sigma}_2 = \left(\beta, \gamma, \delta, \left\{ x^i \right\}_{i=0}^{n-1} \right)$$

- The prover is given only $\boldsymbol{\sigma}$
  - He can only compute linear combinations of the exponents

Proof Generation and Verification

- $\boldsymbol{\pi} \leftarrow \text{Prove}(R, \boldsymbol{\sigma}, a_1, \ldots, a_M)$
  Pick $r, s \leftarrow \mathbb{Z}_p$ and compute $([A]_1, [B]_2, [C]_1)$ where

$$A = \alpha + \sum_{i=0}^{m} a_i u_i(x) + r\delta, \qquad B = \beta + \sum_{i=0}^{m} a_i v_i(x) + s\delta$$

$$C = \frac{\sum_{i=l+1}^{m} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right) + h(x)t(x)}{\delta} + As + Br - rs\delta$$

- $0/1 \leftarrow \text{Verify}(R, \boldsymbol{\sigma}, a_1, \ldots, a_l, \boldsymbol{\pi})$: Check if
  Use the pairing $e : G_1 \times G_2 \rightarrow G_T$ to check that

$$e([A]_1, [B]_2) = e([\alpha]_1, [\beta]_2) \cdot e\left(\left[\frac{\sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\gamma}\right]_1, [\gamma]_2\right) \cdot e([C]_1, [\delta]_2)$$

Zero-Knowledge

- Recall that the setup involved picking $\alpha, \beta, \gamma, \delta, x \leftarrow \mathbb{Z}_p^*$ and setting

$$\boldsymbol{\tau} = (\alpha, \beta, \gamma, \delta, x)$$

- This $\boldsymbol{\tau}$ is the **simulation trapdoor**
- The simulator does the following
  - Pick $A, B \leftarrow \mathbb{Z}_p$
  - Compute

$$C = \frac{AB - \alpha\beta - \sum_{i=0}^{l} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)}{\delta}$$

  - Compute the simulated proof as $([A]_1, [B]_2, [C]_1)$
- $\boldsymbol{\tau}$ is generated using a trusted setup which discards it after generating $\boldsymbol{\sigma} = ([\boldsymbol{\sigma}_1]_1, [\boldsymbol{\sigma}_2]_2)$

$$\boldsymbol{\sigma}_1 = \left(\alpha, \beta, \gamma, \delta, \left\{x^i\right\}_{i=0}^{n-1}, \left\{\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}\right\}_{i=0}^{l}, \right.$$
$$\left. \left\{\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta}\right\}_{i=l+1}^{m}, \left\{\frac{x^i t(x)}{\delta}\right\}_{i=0}^{n-2}\right)$$

$$\boldsymbol{\sigma}_2 = \left(\beta, \gamma, \delta, \left\{x^i\right\}_{i=0}^{n-1}\right)$$

References

- Chapter 2 of My Bitcoin notes
  `https://www.ee.iitb.ac.in/~sarva/bitcoin.html`
- Groth16 paper `https://eprint.iacr.org/2016/260`
- Articles about Groth16
  - Rareskills `https://www.rareskills.io/post/groth16`
  - LambdaClass `https://blog.lambdaclass.com/groth16/`