Split Prover Zero-Knowledge SNARKs

Sanjam Garg

UC Berkeley

Aarushi Goel

Purdue University

Dimitris Kolonelos

UC Berkeley

Sina Shiehian

Snap Inc.

Rohit Sinha

Swirlds Labs

PKC 2025,Røros
12 May 2025

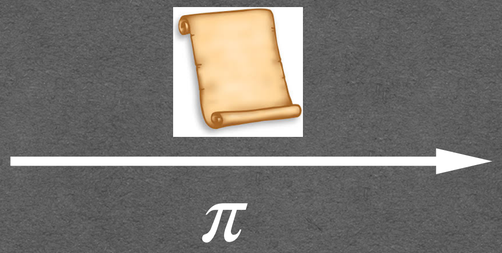
(Zero-Knowledge) SNARKs [Kil92], [Mic94]

zkSNARKs: zero-knowledge Succinct Non-interactive Arguments of Knowledge

$$\mathcal{L} = \{(x; w) : R(x, w) = 1\},\ R \text{ an NP-relation}$$

$\mathcal{P}(x, w)$

$\pi \leftarrow \mathsf{Prove}(x, w)$



π

$\mathcal{V}(x)$

$\mathsf{Verify}(x, \pi) = 1$

- Argument of Knowledge: if $\mathsf{Verify}(x, \pi) = 1$ then $\mathcal{P}$ knows a w s.t. $R(x, w) = 1$
- Zero-Knowledge: $\mathcal{V}$ learns nothing about w
- Non-interactive: $\mathcal{P}$ generates π without any interaction with $\mathcal{V}$
- Succinct: $\|\pi\| \ll \|w\|$ and $\mathsf{Time}(\mathsf{Verify}) \ll \|w\|$

Anonymous Payments and Delegation

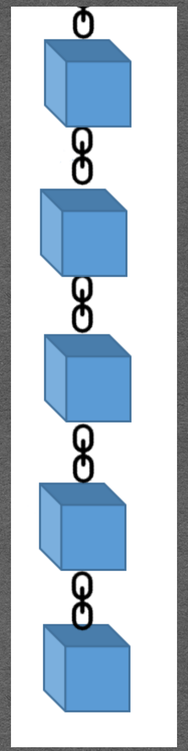
Zerocash [BSCGGMTV14]: Tx=zkSNARK proof

Blockchain

Spender

π

w_1=sk || price || receiver || …



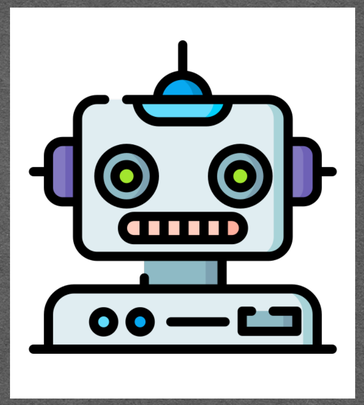
Anonymous Payments and Delegation

Zerocash [BSCGGMTV14]: Tx=zkSNARK proof

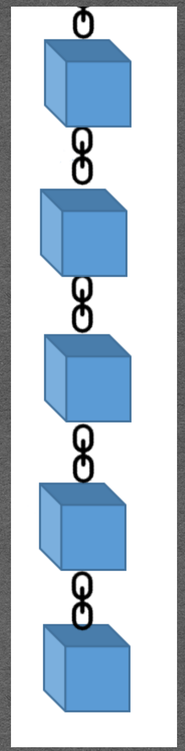
Blockchain

Spender

Delegatee



π



w_1=sk || price || ?? || …

w_2=receiver

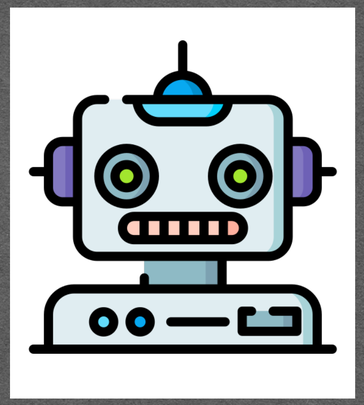
Anonymous Payments and Delegation

Zerocash [BSCGGMTV14]: Tx=zkSNARK proof

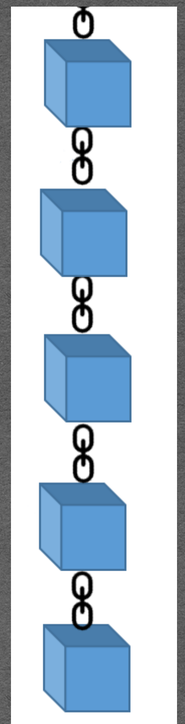
Blockchain

Spender

Delegatee



π



w_1=sk || price || ?? || …

w_2=receiver

Delegatee should not learn w_1

Our Contributions

- **New Notion:** Split Prover zkSNARKs
- **Construction:** Split Prover for Groth16
- **Lower Bound:** For the (Second) Prover Computation

Split Prover zkSNARKs

$$x = x_1 \| x_2 \quad w = w_1 \| w_2$$

Split Prover $(\mathscr{P}_1, \mathscr{P}_2)$

$\mathscr{P}_1(x_1, w_1)$

$\mathscr{P}_2(x_2, w_2)$

$\mathscr{V}(x)$

Split Prover zkSNARKs

$$x = x_1 \| x_2 \quad w = w_1 \| w_2$$

Split Prover $(\mathscr{P}_1, \mathscr{P}_2)$

$\mathscr{P}_1(x_1, w_1)$

aux

$\mathscr{P}_2(x_2, w_2)$

$\mathscr{V}(x)$

aux $\leftarrow$ Prove$_1(x_1, w_1)$

Split Prover zkSNARKs

$$x = x_1 \| x_2 \quad w = w_1 \| w_2$$

Split Prover $(\mathscr{P}_1, \mathscr{P}_2)$

$\mathscr{P}_1(x_1, w_1)$

aux

$\mathscr{P}_2(x_2, w_2)$

π

$\mathscr{V}(x)$

$\text{aux} \leftarrow \text{Prove}_1(x_1, w_1)$

$\pi \leftarrow \text{Prove}_2(x_2, w_2, \text{aux})$

Split Prover zkSNARKs

$$x = x_1 \| x_2 \quad w = w_1 \| w_2$$

Split Prover $(\mathscr{P}_1, \mathscr{P}_2)$

$\mathscr{P}_1(x_1, w_1)$

$\mathscr{P}_2(x_2, w_2)$

$\mathscr{V}(x)$

aux

π

$\text{aux} \leftarrow \text{Prove}_1(x_1, w_1)$

$\pi \leftarrow \text{Prove}_2(x_2, w_2, \text{aux})$

$\text{Verify}(x, \pi) = 1$

Split Prover zkSNARKs

$$x = x_1 \| x_2 \quad w = w_1 \| w_2$$

Split Prover $(\mathscr{P}_1, \mathscr{P}_2)$

$\mathscr{P}_1(x_1, w_1)$

$\mathscr{P}_2(x_2, w_2)$

$\mathscr{V}(x)$

aux

π

$\text{aux} \leftarrow \text{Prove}_1(x_1, w_1)$

$\pi \leftarrow \text{Prove}_2(x_2, w_2, \text{aux})$

$\text{Verify}(x, \pi) = 1$

An (existing) zkSNARK admits a **Split Prover** if it holds:

- **Split Correctness**
- **Split zk:** aux should leak nothing about w_1

But isn't this IVC?

Recursive zkSNARKs

$\mathcal{P}_1(w_1) \xrightarrow{\pi_1} \mathcal{P}_2(w_2) \xrightarrow{\pi_2}$

$R_1(x_1, w_1)$ $R_1(x_2, w_2) \wedge \mathsf{Verify}(\pi_1)$

Split Prover zkSNARKs

$\mathcal{P}_1(w_1) \xrightarrow{\text{aux}} \mathcal{P}_2(w_2) \xrightarrow{\pi}$

$R(x, w)$

But isn't this IVC?

Recursive zkSNARKs

- Non-Black Box
- Heurstic Assumption
- Verifier Changes

$\mathcal{P}_1(w_1) \xrightarrow{\pi_1} \mathcal{P}_2(w_2) \xrightarrow{\pi_2}$

$R_1(x_1, w_1)$ $R_1(x_2, w_2) \wedge \text{Verify}(\pi_1)$

Split Prover zkSNARKs

Goals:

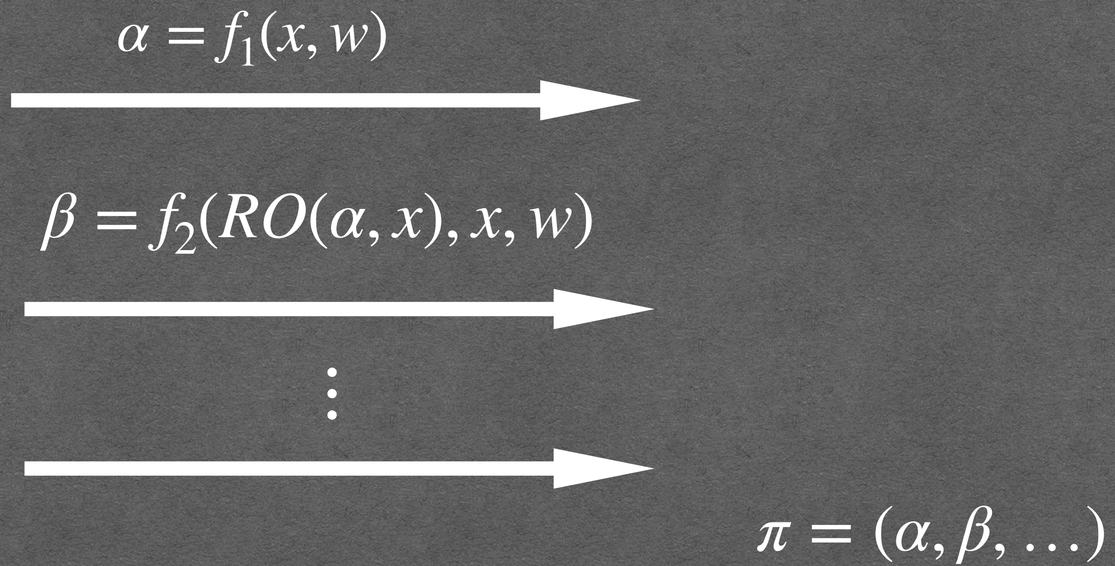
- Black Box
- Provable Security
- Same verification algorithm

$\mathcal{P}_1(w_1) \xrightarrow{\text{aux}} \mathcal{P}_2(w_2) \xrightarrow{\pi}$

$R(x, w)$

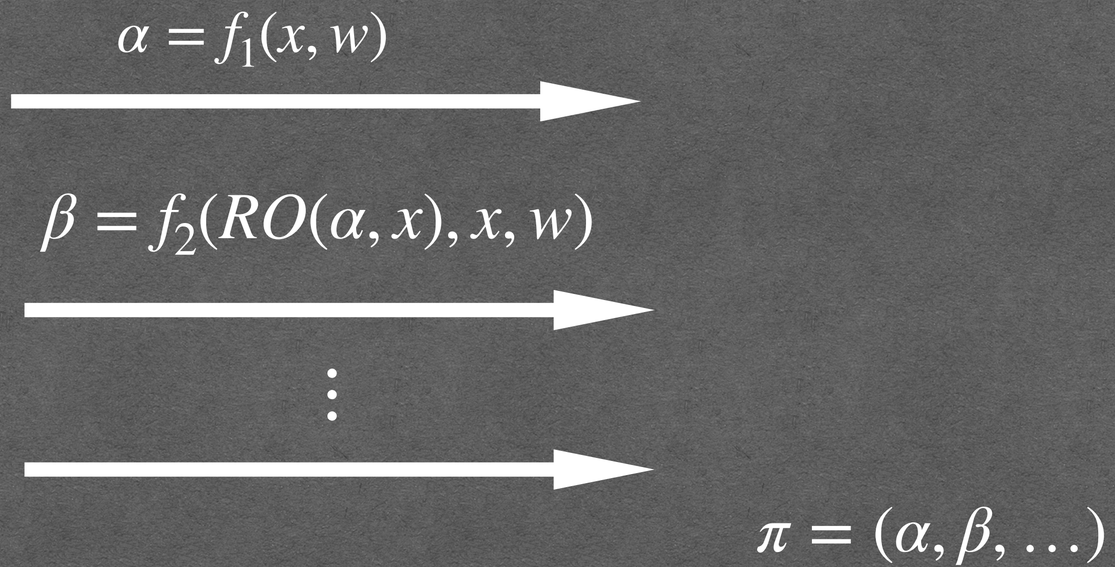
Barriers on Constructions

Fiat-Shamir (RO) based SNARKS (PLONK, Bulletproofs, STARKs, …)



Barriers on Constructions

Fiat-Shamir (RO) based SNARKS (PLONK, Bulletproofs, STARKs, …)



Observation: Groth16 does not use Fiat-Shamir

Our Solution

Warning: *Technical Slides Ahead* 

Groth16 in a nutshell

R1CS relations:

Hadamard Product

$$\begin{pmatrix} a_{11} & a_{21} & a_{31} & a_{41} \\ a_{12} & a_{22} & a_{32} & a_{42} \\ a_{13} & a_{23} & a_{33} & a_{43} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} \bullet \begin{pmatrix} b_{11} & b_{21} & b_{31} & b_{41} \\ b_{12} & b_{22} & b_{32} & b_{42} \\ b_{13} & b_{23} & b_{33} & b_{43} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} c_{11} & c_{21} & c_{31} & c_{41} \\ c_{12} & c_{22} & c_{32} & c_{42} \\ c_{13} & c_{23} & c_{33} & c_{43} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix}$$

$$R = \{(\mathbf{x}, \mathbf{w}) : \mathbf{Az} \circ \mathbf{Bz} = \mathbf{Cz} \ \wedge \ \mathbf{z} = \mathbf{x} \| \mathbf{w}\}$$

Groth16 in a nutshell

R1CS relations:

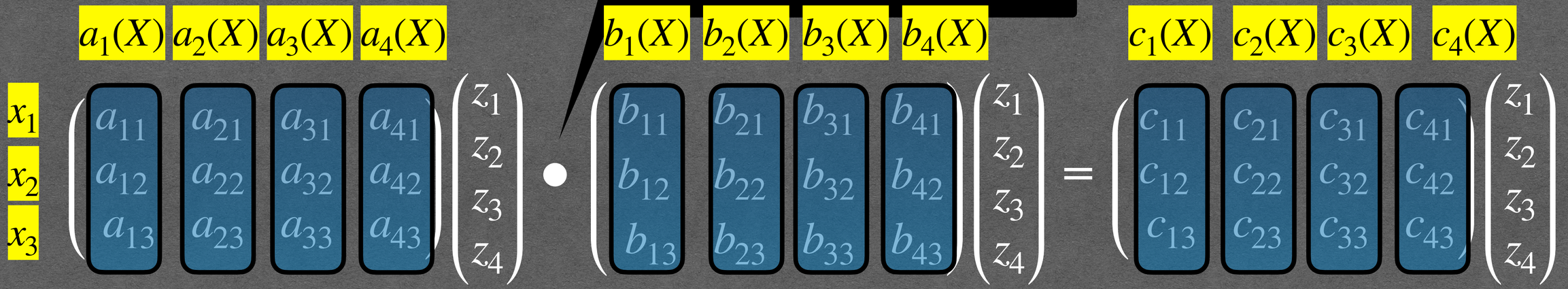
Hadamard Product

$$\begin{matrix} x_1 \\ x_2 \\ x_3 \end{matrix} \begin{pmatrix} a_{11} & a_{21} & a_{31} & a_{41} \\ a_{12} & a_{22} & a_{32} & a_{42} \\ a_{13} & a_{23} & a_{33} & a_{43} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} \bullet \begin{pmatrix} b_{11} & b_{21} & b_{31} & b_{41} \\ b_{12} & b_{22} & b_{32} & b_{42} \\ b_{13} & b_{23} & b_{33} & b_{43} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} c_{11} & c_{21} & c_{31} & c_{41} \\ c_{12} & c_{22} & c_{32} & c_{42} \\ c_{13} & c_{23} & c_{33} & c_{43} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix}$$

$$R = \{(\mathbf{x}, \mathbf{w}) : \mathbf{Az} \circ \mathbf{Bz} = \mathbf{Cz} \ \wedge \ \mathbf{z} = \mathbf{x} \| \mathbf{w}\}$$

Groth16 in a nutshell

R1CS relations:



$$R = \{(\mathbf{x}, \mathbf{w}) : \mathbf{Az} \circ \mathbf{Bz} = \mathbf{Cz} \ \wedge \ \mathbf{z} = \mathbf{x} \| \mathbf{w}\}$$

Groth16 in a nutshell

R1CS relations:

Hadamard Product

$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array}\begin{array}{c} \begin{matrix} a_1(X) & a_2(X) & a_3(X) & a_4(X) \end{matrix} \\ \begin{pmatrix} a_{11} & a_{21} & a_{31} & a_{41} \\ a_{12} & a_{22} & a_{32} & a_{42} \\ a_{13} & a_{23} & a_{33} & a_{43} \end{pmatrix} \end{array}\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} \bullet \begin{array}{c} \begin{matrix} b_1(X) & b_2(X) & b_3(X) & b_4(X) \end{matrix} \\ \begin{pmatrix} b_{11} & b_{21} & b_{31} & b_{41} \\ b_{12} & b_{22} & b_{32} & b_{42} \\ b_{13} & b_{23} & b_{33} & b_{43} \end{pmatrix} \end{array}\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{array}{c} \begin{matrix} c_1(X) & c_2(X) & c_3(X) & c_4(X) \end{matrix} \\ \begin{pmatrix} c_{11} & c_{21} & c_{31} & c_{41} \\ c_{12} & c_{22} & c_{32} & c_{42} \\ c_{13} & c_{23} & c_{33} & c_{43} \end{pmatrix} \end{array}\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix}$$

$$R = \{(\mathbf{x}, \mathbf{w}) : \mathbf{Az} \circ \mathbf{Bz} = \mathbf{Cz} \ \wedge \ \mathbf{z} = \mathbf{x}$$

Vanishing Polynomial $V(X)$

R1CS satisfiability:

$$\left(\sum_{i=1}^{4} z_i a_i(X)\right)\left(\sum_{i=1}^{4} z_i b_i(X)\right) - \left(\sum_{i=1}^{4} z_i c_i(X)\right) = q(X)\prod_{i=1}^{3}(X - x_i)$$

Groth16 in a nutshell

$$[x]_i := g_i^x \in \mathbb{G}_i$$

R1CS satisfiability:

$$\left(\sum_{i=1}^{m} z_i a_i(X)\right) \cdot \left(\sum_{i=1}^{m} z_i b_i(X)\right) - \left(\sum_{i=1}^{m} z_i c_i(X)\right) = q(X)V(X)$$

Cryptographic realization (with pairings):

Groth16 in a nutshell

$$[x]_i := g_i^x \in \mathbb{G}_i$$

R1CS satisfiability:

$$\left(\sum_{i=1}^{m} z_i a_i(X)\right) \cdot \left(\sum_{i=1}^{m} z_i b_i(X)\right) - \left(\sum_{i=1}^{m} z_i c_i(X)\right) = q(X)V(X)$$

Cryptographic realization (with pairings):

$$\pi_1 = [\alpha]_1 + \sum_{i=1}^{m} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1 \qquad \pi_2 = [\beta]_2 + \sum_{i=1}^{m} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

Groth16 in a nutshell

$$[x]_i := g_i^x \in \mathbb{G}_i$$

R1CS satisfiability:

$$\left(\sum_{i=1}^{m} z_i a_i(X)\right) \cdot \left(\sum_{i=1}^{m} z_i b_i(X)\right) - \left(\sum_{i=1}^{m} z_i c_i(X)\right) = q(X)V(X)$$

Cryptographic realization (with pairings):

$$\pi_1 = [\alpha]_1 + \sum_{i=1}^{m} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1 \qquad \pi_2 = [\beta]_2 + \sum_{i=1}^{m} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

$$\pi_3 = \sum_{i=1}^{m} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1 + s\sum_{i=1}^{m} z_i \cdot [a_i(x)]_1 + r\sum_{i=1}^{m} z_i \cdot [b_i(x)]_1$$

$$+ \sum_{i=0}^{n-2} \widetilde{q}_i \cdot \left[\frac{V(x)x^i}{\delta}\right]_1 + s \cdot [\alpha]_1 + r \cdot [\beta]_1 + rs \cdot [\delta]_1$$

Groth16 in a nutshell

$$[x]_i := g_i^x \in \mathbb{G}_i$$

R1CS satisfiability:

$$\left(\sum_{i=1}^{m} z_i a_i(X)\right) \cdot \left(\sum_{i=1}^{m} z_i b_i(X)\right) - \left(\sum_{i=1}^{m} z_i c_i(X)\right) = q(X)V(X)$$

Cryptographic realization (with pairings):

$$\pi_1 = [\alpha]_1 + \sum_{i=1}^{m} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1 \qquad \pi_2 = [\beta]_2 + \sum_{i=1}^{m} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

$$\pi_3 = \sum_{i=1}^{m} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1 + s \sum_{i=1}^{m} z_i \cdot [a_i(x)]_1 + r \sum_{i=1}^{m} z_i \cdot [b_i(x)]_1$$

$$+ \sum_{i=0}^{n-2} \tilde{q}_i \cdot \left[\frac{V(x)x^i}{\delta}\right]_1 + s \cdot [\alpha]_1 + r \cdot [\beta]_1 + rs \cdot [\delta]_1$$

Groth16 in a nutshell

$$[x]_i := g_i^x \in \mathbb{G}_i$$

R1CS satisfiability:

$$\left(\sum_{i=1}^{m} z_i a_i(X)\right) \cdot \left(\sum_{i=1}^{m} z_i b_i(X)\right) - \left(\sum_{i=1}^{m} z_i c_i(X)\right) = q(X)V(X)$$

Witness

Cryptographic realization (with pairings):

$$\pi_1 = [\alpha]_1 + \sum_{i=1}^{m} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1 \qquad \pi_2 = [\beta]_2 + \sum_{i=1}^{m} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

$$\pi_3 = \sum_{i=1}^{m} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1 + s \sum_{i=1}^{m} z_i \cdot [a_i(x)]_1 + r \sum_{i=1}^{m} z_i \cdot [b_i(x)]_1$$

$$+ \sum_{i=0}^{n-2} \tilde{q}_i \cdot \left[\frac{V(x)x^i}{\delta}\right]_1 + s \cdot [\alpha]_1 + r \cdot [\beta]_1 + rs \cdot [\delta]_1$$

Groth16 in a nutshell

$$[x]_i := g_i^x \in \mathbb{G}_i$$

R1CS satisfiability:

$$\left(\sum_{i=1}^{m} z_i a_i(X)\right) \cdot \left(\sum_{i=1}^{m} z_i b_i(X)\right) - \left(\sum_{i=1}^{m} z_i c_i(X)\right) = q(X)V(X)$$

Witness

Cryptographic realization (with pairings):

$$\pi_1 = [\alpha]_1 + \sum_{i=1}^{m} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1$$

$$\pi_2 = [\beta]_2 + \sum_{i=1}^{m} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

$$\pi_3 = \sum_{i=1}^{m} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1 + s\sum_{i=1}^{m} z_i \cdot [a_i(x)]_1 + r\sum_{i=1}^{m} z_i \cdot [b_i(x)]_1$$

$$+ \sum_{i=0}^{n-2} \tilde{q}_i \cdot \left[\frac{V(x)x^i}{\delta}\right]_1 + s \cdot [\alpha]_1 + r \cdot [\beta]_1 + rs \cdot [\delta]_1$$

Split Prover for Groth16 (1)

Split R1CS

Let $\mathbf{z} = \mathbf{z}_I \| \mathbf{z}_{II}$ then:

$$\begin{pmatrix} a_{11} & a_{21} & a_{31} & a_{41} \\ a_{12} & a_{22} & a_{32} & a_{42} \\ a_{13} & a_{23} & a_{33} & a_{43} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} \bullet \begin{pmatrix} b_{11} & b_{21} & b_{31} & b_{41} \\ b_{12} & b_{22} & b_{32} & b_{42} \\ b_{13} & b_{23} & b_{33} & b_{43} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} c_{11} & c_{21} & c_{31} & c_{41} \\ c_{12} & c_{22} & c_{32} & c_{42} \\ c_{13} & c_{23} & c_{33} & c_{43} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix}$$

Split Prover for Groth16 (1)

Split R1CS

Let $\mathbf{z} = \mathbf{z}_I \| \mathbf{z}_{II}$ then:

$$\left(\begin{array}{ccc|c} a_{11} & a_{21} & a_{31} & a_{41} \\ a_{12} & a_{22} & a_{32} & a_{42} \\ a_{13} & a_{23} & a_{33} & a_{43} \end{array}\right)\left(\begin{array}{c} z_1 \\ z_2 \\ z_3 \\ \hline z_4 \end{array}\right) \bullet \left(\begin{array}{ccc|c} b_{11} & b_{21} & b_{31} & b_{41} \\ b_{12} & b_{22} & b_{32} & b_{42} \\ b_{13} & b_{23} & b_{33} & b_{43} \end{array}\right)\left(\begin{array}{c} z_1 \\ z_2 \\ z_3 \\ \hline z_4 \end{array}\right) = \left(\begin{array}{ccc|c} c_{11} & c_{21} & c_{31} & c_{41} \\ c_{12} & c_{22} & c_{32} & c_{42} \\ c_{13} & c_{23} & c_{33} & c_{43} \end{array}\right)\left(\begin{array}{c} z_1 \\ z_2 \\ z_3 \\ \hline z_4 \end{array}\right)$$

$$\begin{pmatrix} \mathbf{A}_I & \mathbf{A}_{II} \end{pmatrix}\begin{pmatrix} \mathbf{z}_I \\ \mathbf{z}_{II} \end{pmatrix} \bullet \begin{pmatrix} \mathbf{B}_I & \mathbf{B}_{II} \end{pmatrix}\begin{pmatrix} \mathbf{z}_I \\ \mathbf{z}_{II} \end{pmatrix} = \begin{pmatrix} \mathbf{C}_I & \mathbf{C}_{II} \end{pmatrix}\begin{pmatrix} \mathbf{z}_I \\ \mathbf{z}_{II} \end{pmatrix}$$

Split Prover for Groth16 (1)

Split R1CS

Let $\mathbf{z} = \mathbf{z}_I \| \mathbf{z}_{II}$ then:

$$\left(\begin{array}{ccc|c} a_{11} & a_{21} & a_{31} & a_{41} \\ a_{12} & a_{22} & a_{32} & a_{42} \\ a_{13} & a_{23} & a_{33} & a_{43} \end{array}\right)\left(\begin{array}{c} z_1 \\ z_2 \\ z_3 \\ \hline z_4 \end{array}\right) \bullet \left(\begin{array}{ccc|c} b_{11} & b_{21} & b_{31} & b_{41} \\ b_{12} & b_{22} & b_{32} & b_{42} \\ b_{13} & b_{23} & b_{33} & b_{43} \end{array}\right)\left(\begin{array}{c} z_1 \\ z_2 \\ z_3 \\ \hline z_4 \end{array}\right) = \left(\begin{array}{ccc|c} c_{11} & c_{21} & c_{31} & c_{41} \\ c_{12} & c_{22} & c_{32} & c_{42} \\ c_{13} & c_{23} & c_{33} & c_{43} \end{array}\right)\left(\begin{array}{c} z_1 \\ z_2 \\ z_3 \\ \hline z_4 \end{array}\right)$$

$$\begin{pmatrix} \mathbf{A}_I & \mathbf{A}_{II} \end{pmatrix}\begin{pmatrix} \mathbf{z}_I \\ \mathbf{z}_{II} \end{pmatrix} \bullet \begin{pmatrix} \mathbf{B}_I & \mathbf{B}_{II} \end{pmatrix}\begin{pmatrix} \mathbf{z}_I \\ \mathbf{z}_{II} \end{pmatrix} = \begin{pmatrix} \mathbf{C}_I & \mathbf{C}_{II} \end{pmatrix}\begin{pmatrix} \mathbf{z}_I \\ \mathbf{z}_{II} \end{pmatrix}$$

$$\Rightarrow (\mathbf{A}_I\mathbf{z}_I \bullet \mathbf{B}_I\mathbf{z}_I) + (\mathbf{A}_I\mathbf{z}_I \bullet \mathbf{B}_{II}\mathbf{z}_{II}) + (\mathbf{A}_{II}\mathbf{z}_{II} \bullet \mathbf{B}_1\mathbf{z}_1) + (\mathbf{A}_{II}\mathbf{z}_{II} \bullet \mathbf{B}_{II}\mathbf{z}_{II}) = (\mathbf{C}_I\mathbf{z}_I) + (\mathbf{C}_{II}\mathbf{z}_{II})$$

Split Prover Groth16 (2)

$$\pi_1 = [\alpha]_1 + \sum_{i \in I} z_i \cdot [a_i(x)]_1 + \sum_{i \in II} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1$$

$$\pi_2 = [\beta]_2 + \sum_{i \in I} z_i \cdot [b_i(x)]_2 + \sum_{i \in II} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

Split Prover Groth16 (2)

$$\pi_1 = [\alpha]_1 + \sum_{i \in I} z_i \cdot [a_i(x)]_1 + \sum_{i \in II} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1$$

$$\pi_2 = [\beta]_2 + \sum_{i \in I} z_i \cdot [b_i(x)]_2 + \sum_{i \in II} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

Split Prover Groth16 (2)

$$\pi_1 = [\alpha]_1 + \sum_{i \in I} z_i \cdot [a_i(x)]_1 + \sum_{i \in II} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1$$

$$\pi_2 = [\beta]_2 + \sum_{i \in I} z_i \cdot [b_i(x)]_2 + \sum_{i \in II} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

Split Prover Groth16 (2)

$$\pi_1 = [\alpha]_1 + \sum_{i \in I} z_i \cdot [a_i(x)]_1 + \sum_{i \in II} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1$$

$$\pi_2 = [\beta]_2 + \sum_{i \in I} z_i \cdot [b_i(x)]_2 + \sum_{i \in II} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

$$\pi_3 = \sum_{i \in I} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1 + \sum_{i \in II} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1$$

$$+ s\left(\sum_{i \in I} z_i \cdot [a_i(x)]_1 + \sum_{i \in II} z_i \cdot [a_i(x)]_1\right) + r\left(\sum_{i \in I} z_i \cdot [b_i(x)]_1 + \sum_{i \in II} z_i \cdot [b_i(x)]_1\right)$$

$$+ \sum_{i=0}^{n-2} \widetilde{q}_i \cdot \left[\frac{V(x)x^i}{\delta}\right]_1 + s \cdot [\alpha]_1 + r \cdot [\beta]_1 + rs \cdot [\delta]_1$$

Split Prover Groth16 (2)

$$\pi_1 = [\alpha]_1 + \sum_{i \in I} z_i \cdot [a_i(x)]_1 + \sum_{i \in II} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1$$

$$\pi_2 = [\beta]_2 + \sum_{i \in I} z_i \cdot [b_i(x)]_2 + \sum_{i \in II} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

$$\pi_3 = \sum_{i \in I} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1 + \sum_{i \in II} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1$$
$$+ s\left(\sum_{i \in I} z_i \cdot [a_i(x)]_1 + \sum_{i \in II} z_i \cdot [a_i(x)]_1\right) + r\left(\sum_{i \in I} z_i \cdot [b_i(x)]_1 + \sum_{i \in II} z_i \cdot [b_i(x)]_1\right)$$
$$+ \sum_{i=0}^{n-2} \tilde{q}_i \cdot \left[\frac{V(x)x^i}{\delta}\right]_1 + s \cdot [\alpha]_1 + r \cdot [\beta]_1 + rs \cdot [\delta]_1$$

Split Prover Groth16 (2)

$$\pi_1 = [\alpha]_1 + \sum_{i \in I} z_i \cdot [a_i(x)]_1 + \sum_{i \in II} z_i \cdot [a_i(x)]_1 + r \cdot [\delta]_1$$

$$\pi_2 = [\beta]_2 + \sum_{i \in I} z_i \cdot [b_i(x)]_2 + \sum_{i \in II} z_i \cdot [b_i(x)]_2 + s \cdot [\delta]_2$$

$$\pi_3 = \sum_{i \in I} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1 + \sum_{i \in II} z_i \cdot \left[\frac{\beta a_i(x) + \alpha b_i(x) + c_i(x)}{\delta}\right]_1$$
$$+ s\left(\sum_{i \in I} z_i \cdot [a_i(x)]_1 + \sum_{i \in II} z_i \cdot [a_i(x)]_1\right) + r\left(\sum_{i \in I} z_i \cdot [b_i(x)]_1 + \sum_{i \in II} z_i \cdot [b_i(x)]_1\right)$$
$$+ \sum_{i=0}^{n-2} \tilde{q}_i \cdot \left[\frac{V(x)x^i}{\delta}\right]_1 + s \cdot [\alpha]_1 + r \cdot [\beta]_1 + rs \cdot [\delta]_1$$

Split Prover Groth16 (3)

Observation: The quotient can also be split

$$q(X) = \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)} +$$
$$\frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)}$$

Split Prover Groth16 (3)

Observation: The quotient can also be split

$$q(X) = \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)}$$

Split Prover Groth16 (3)

Observation: The quotient can also be split

$$q(X) = \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)}$$

$$q_2(X) = \frac{\left\langle \vec{z}_I, \vec{a}_I(X)\right\rangle \cdot \left\langle \vec{z}_{II}, \vec{a}_{II}(X)\right\rangle}{V(X)} = \left\langle \vec{z}_{II}\ , \frac{\left\langle \vec{z}_I, \vec{a}_I(X)\right\rangle \cdot \vec{b}_{II}(X)}{V(X)} \right\rangle$$

Split Prover Groth16 (3)

Observation: The quotient can also be split

$$q(X) = \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)}$$

$$q_2(X) = \frac{\langle \vec{z}_I, \vec{a}_I(X)\rangle \cdot \langle \vec{z}_{II}, \vec{a}_{II}(X)\rangle}{V(X)} = \left\langle \vec{z}_{II}, \frac{\langle \vec{z}_I, \vec{a}_I(X)\rangle \cdot \vec{b}_{II}(X)}{V(X)} \right\rangle$$

Split Prover Groth16 (3)

Observation: The quotient can also be split

$$q(X) = \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in I} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in I} z_i b_i(X)\right)}{V(X)} + \frac{\left(\sum_{i\in II} z_i a_i(X)\right)\left(\sum_{i\in II} z_i b_i(X)\right)}{V(X)}$$

$$q_2(X) = \frac{\langle \vec{z}_I, \vec{a}_I(X)\rangle \cdot \langle \vec{z}_{II}, \vec{a}_{II}(X)\rangle}{V(X)} = \left\langle \vec{z}_{II}, \frac{\langle \vec{z}_I, \vec{a}_I(X)\rangle \cdot \vec{b}_{II}(X)}{V(X)} \right\rangle$$

Similarly for $q_3(X)$...

More in the paper

- **Split zk**: aux *should be randomized*

  ➡ Common trick (e.g. see Ligero [AHIV17]): Add 3 dummy artificial constraints and choose the corresponding z_1, z_2, z_3 at random to 'blind' aux.

- **Impossibility Result**: *For any Split Prover realization for Groth16, $\mathscr{P}_{II}$ must perform at least* $\Omega(\mathsf{Min}\{n-1, \mathsf{rank}(\mathbf{A}_{II}) \cdot \mathsf{rank}(\mathbf{B}_{II})\})$ *group operations.*

  ➡ Our $\mathscr{P}_{II}$ Split Prover is tight.

Conclusions

Recap:

- Split Prover zkSNARKs as an alternative to IVC
- Split Prover for Groth16
- Proof of tightness of prover's computation

Future Directions:

- n-prover Split Prover zkSNARKs
- Sublinear second prover
- Applications (Anonymous payment delegation, Anonyous credentials)

Thank you!