Snarks and R1CS

Tuesday, November 14, 2017 12:32 PM

$ZK\{(a): A = g^a \text{ and } A' = g^{a^2}\}$ $\quad (\log_g A)^2 = (\log_g A)$

$k_1 \xleftarrow{\$} \mathbb{Z}_p,\ k_2 \xleftarrow{\$} \mathbb{Z}_p \quad A' = A^a$

$K_1 := g^{k_1}$

$K_2 := g^{k_2 a}$

$K_1, K_2 \longrightarrow$

$\longleftarrow c$

$s_1 = k_1 - ca$

$s_2 = k_2 - ca$ $\quad s_1, s_2 \longrightarrow$

$ZK\{(a_1, a_2): A = g^{a_1},\ A' = g^{a_2^2}\}$

Rank 1 Constraint System: over a set of variables $\vec{a} = (a_0, a_1, \ldots a_m) \in \mathbb{F}^m$

(R1CS) where $a_0 = 1$

defined by

- N equations of the form:

ex. 1) $(a_1 + 4a_2 + a_3) \cdot (a_1 + 8a_7) = (5a_6)$

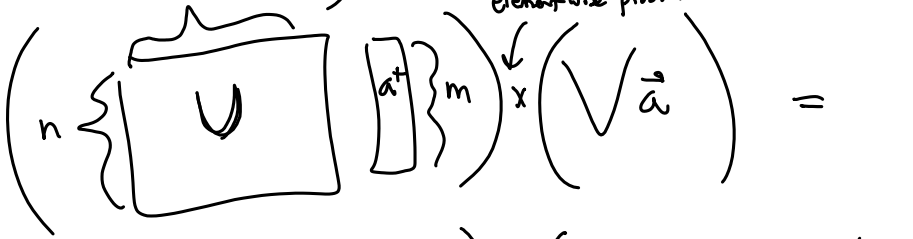
2)

:

N)

- or by matrices $U, V, W \in \mathbb{F}^{n \times m}$

$$(U\vec{a}^T) \cdot (V\vec{a}^T) = (W\vec{a}^T)$$



$$\forall_{j \le N} \left(\sum_i U_{j,i} \cdot a_i\right) \cdot \left(\sum_i V_{j,i} \cdot a_i\right) = \left(\sum_i W_{j,i} \cdot a_i\right)$$

We can have efficient ZK ("Snarks") for all R1CS

$$ZK\{(a_{m'+1}, \ldots a_m) : \underline{U}\,\bar{a} \cdot \underline{V}\,\bar{a} = \underline{W}\,\bar{a}\}$$

(statement: $a_{m'+1}, \ldots a_m$; witness: $\bar{a}$)

$$\bar{a} = (a_1, \ldots a_{m'}, a_{m'+1}, \ldots a_m)$$

($a_1, \ldots a_{m'}$: witness; $a_{m'+1}, \ldots a_m$: statement)

$$ZK_X\{(w) : P(x, w)\}$$

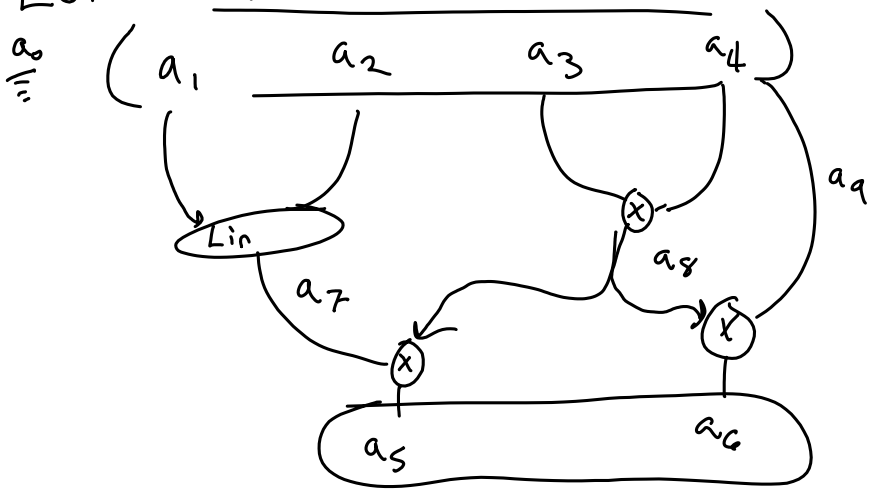
(w: witness; x: statement; $P(x,w)$: predicate "aka statement")

$$ZK\{(a) : A = g^a \; B = g^{a^2}\}$$

(A, B: statement)

RICS:
- "Complete" ie can express arbitrary circuits as RICS
- "Convenient" efficiently compile programs of interest

Let's compile arithmetic circuits to RICS



1) ~~$(a_1 + a_2) \cdot 1 = a_7$~~

2) $(a_3) \cdot (a_4) = a_8$

3) $(a_1 + a_2) \cdot a_8 = a_5$

4) $a_8 \cdot a_9 = a_6$

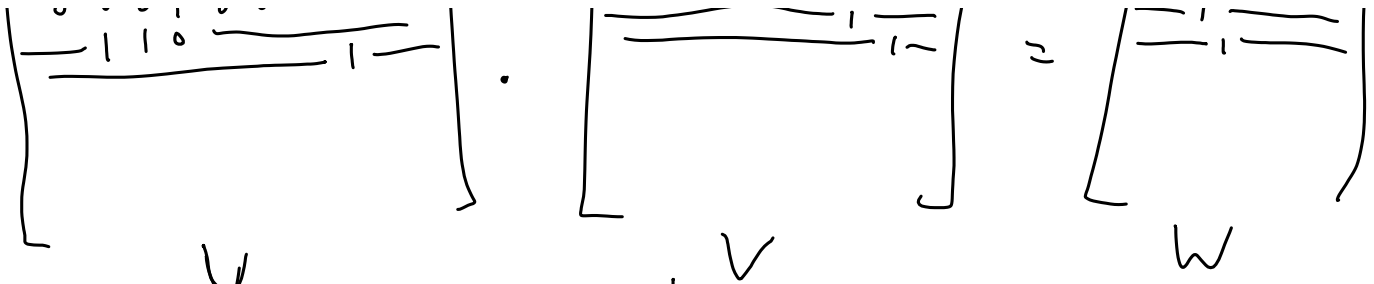
In matrix form

$$\begin{bmatrix} U \end{bmatrix} \cdot \begin{bmatrix} V \end{bmatrix} \cdot \begin{bmatrix} a \end{bmatrix}$$

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 8 & 9 \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

$$\begin{bmatrix} 5 & 6 & 8 \\ \cdot & \cdot & 1 \end{bmatrix}$$



U V W

$F : \mathbb{F}^{|in|} \to \mathbb{F}^{|out|}$

(U,V,W) computes F if

$F(a_1, \ldots a_{|in|}) = (a_{|in|+1}, \ldots a_{|out|+|in|})$ iff

$\exists (a_{|in|+|out|+1}, \ldots a_m)$ s.t. $U\bar{a} \cdot V\bar{a} = W\bar{a}$

$(a_1, \ldots a_{|in|}, a_{|in|+1}, \ldots a_{|out|+|in|}, \ldots a_m)$

inputs outputs internal wires "advice"

Useful gadget: Zero test

$Y = \overset{1}{\text{if}} (X != 0)$ · else 0

$\exists M^{\mathbb{F}}$ $(X) \cdot (M) = Y$ $\quad X=0 \Rightarrow Y=0$

$(1-Y) \cdot (X) = 0$ $\quad X!=0 \Rightarrow Y=1$ $\quad M = 1/X$

$Y = (X == Z)$

$Y_1 = (X - Z) == 0$

Range Proofs / "Split gates"

$X \in [0, 2^k - 1]$

$X_1 \in [0, 1]$ $\quad (X_1 + 2X_2 \ldots 2^k X_k) \cdot 1 = X$

$x_2 \in$

$\alpha_3 \therefore x_K$

$X \in [0,1]$?

$X \cdot (1-X) = 0$ ✓