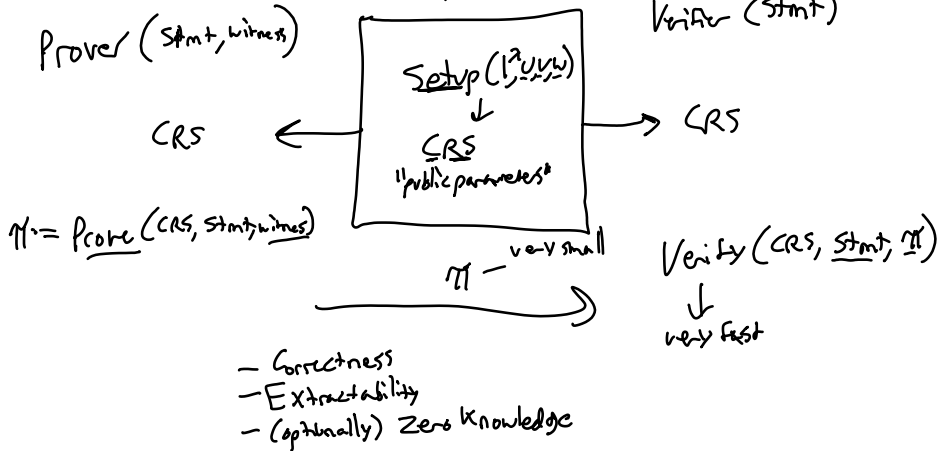


# verifiable computing and the CRS model

Common Reference String

"Trusted Setup"

Start with relations  $R_{CRS}(U, V, W)$



## Trusted Setup:

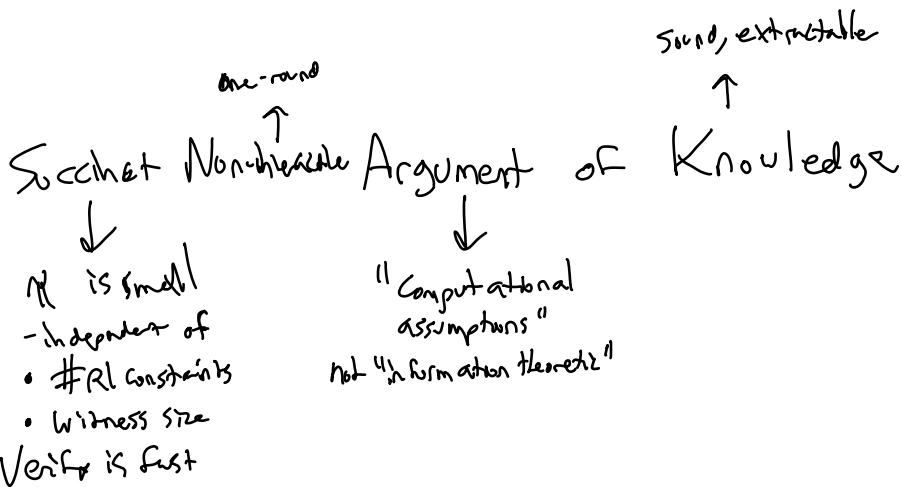
- Like choosing generators for discrete log crypto
- If uniform parameters, should use "NUMS"
- Otherwise, need to flip coins, then forget the coins

Ex.  $\mathbb{P} \leftarrow \mathcal{D}$

$$Setup(I^n):$$

$$\underline{s} \in \mathbb{Z}_p, g \in G \quad \text{for some } n.$$

$$CRS = (g, g^s, g^{s^2}, g^{s^3}, \dots, g^{s^n})$$



## Recall RLCS over a field $F$

$m$  variables  $a_1, \dots, a_m$

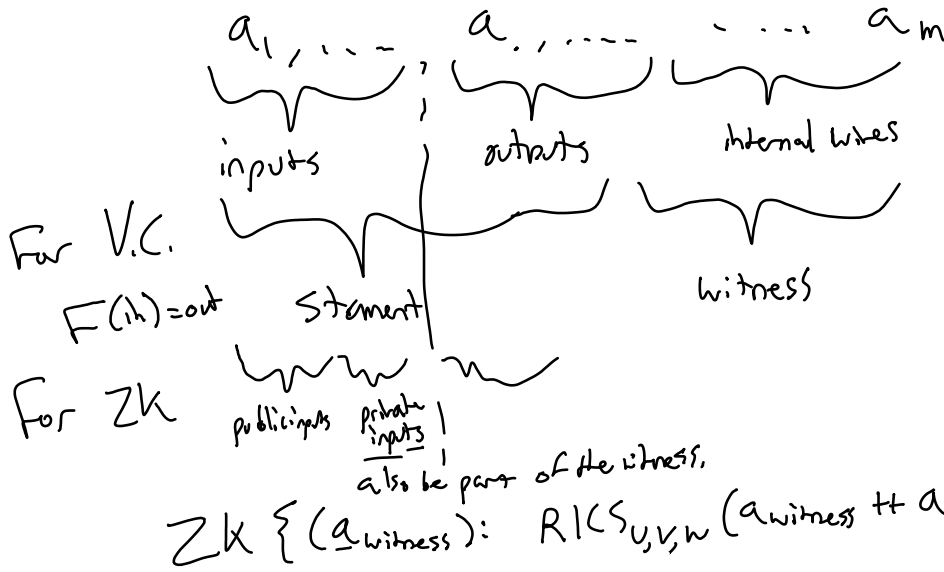
$\{a_i\}$  ranges over  $\{1, \dots, m\}$

also  $a_0 = 1$

$n$  RI constraints  $U, V, W$  are  $m \times n$  matrices of coefficients  $\in \mathbb{F}$

$$(1) \quad \forall a \quad \left( \sum_i U_{i,a} \cdot a_i \right) \cdot \left( \sum_i V_{i,a} \cdot a_i \right) = \left( \sum_i W_{i,a} \cdot a_i \right)$$

Encode computations:



Step 1. Encode  $U, V, W$  as polynomials

Take arbitrary roots  $r_a \quad r_1, \dots, r_n \in \mathbb{F}$   
 Could be  $r_1 = 1, r_2 = 2, \dots$     one for each constraint.

$\forall i$ , Define  $U_i(X)$  by interpolation so that  $U_i(r_a) = U_{i,a}$   
 Same for  $V_i(X)$      $V_i(r_a) = V_{i,a}$   
 $W_i(X)$      $W_i(r_a) = W_{i,a}$   
 $U_i(r_a) = U_{i,a}$      $\uparrow$  each polynomial is degree  $(n-1)$

$$(2) \quad \forall a \quad \left( \sum_i U_i(r_a) \cdot a_i \right) \cdot \left( \sum_i V_i(r_a) \cdot a_i \right) = \left( \sum_i W_i(r_a) \cdot a_i \right)$$

Define  $P(X) = \left( \sum_i U_i(X) \cdot a_i \right) \left( \sum_i V_i(X) \cdot a_i \right) - \left( \sum_i W_i(X) \cdot a_i \right)$

$$(3) \quad \forall a \quad P(r_a) = 0 \quad \leftarrow \text{a degree } 2(n-1) \text{ over } X \text{ with roots at least } n \text{ roots}$$

Define a smaller degree polynomial  $t(X)$  that has the same roots as  $p(X)$

$$t(X) = (X-r_1)(X-r_2)\dots(X-r_n)$$

- has roots at each  $r_i$

- degree  $n$

- "monic" leading coefficient is 1

$$t(X) = X^n + \dots$$

If  $p(X)$  shares  $n$  roots with  $t(X)$ , then  $p(X)$  is a multiple of  $t(X)$ .

$$(4) \quad p(X) \equiv 0 \pmod{t(X)}$$

$$(5) \quad \exists \text{ polynomial } h(X) \text{ s.t. } t(X) \cdot h(X) = p(X)$$

ex  $p(X) = X^4 + \dots$   
 divides by  $t(X) = X^3 + \dots$   
 $p(X) = (5X) \cdot t(X) + (\text{rem}(X))$  degree 3 or less  
 $(5X^4 + \dots)$

$$p(X) = t(X) \cdot h(X) + \text{rem}(X)$$

$\text{deg}(\text{rem}) \ll \text{deg}(p) - \text{deg}(t)$

Step 3) suffices to check  $p(s) = h(s) \cdot t(s)$   
 for a randomly chosen  $s \in \mathbb{F}$ .

Setup:  $u_i(X), v_i(X), w_i(X), t(X)$  only depends on  $r_1, \dots, r_n$

prover computes  $\bar{a}$ ,  $p(X)$  depends on  $u_i(X) \dots w_i$  and on  $\bar{a}$   
 compute  $h(X) = p(X)/t(X)$

Commit  $h, p, \bar{a}$

1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100.

← verifier knows  $u$

Prover evaluate  $\pi = p(s), h(s), t(s)$   
 verifier verify  $p(s) = h(s) \cdot t(s)$

Remaining problem: need to check that  $p(s), \dots$  are done consistently.

Step 3). Setup  $s \leftarrow \mathbb{F}$

map  $u_i(x), v_i(x), w_i(x)$  to elements in  $G$

$$\text{CRS} := \left\{ g^{\frac{u_i(s)}{v_i(s)}} \right\}, \left\{ g^{\frac{v_i(s)}{w_i(s)}} \right\}, \left\{ g^{\frac{w_i(s)}{t(s)}} \right\}, g^{t(s)} \dots$$

Prover computes  $p(x), h(x)$

$$g^{\sum_i u_i(s) \cdot a_i} = \prod_i \left( g^{u_i(s)} \right)^{a_i}$$

Same for  $g^{\sum_i v_i(s) \cdot a_i}$  and  $g^{\sum_i w_i(s) \cdot a_i}$

Also add  $\text{CRS} := \dots g^s, g^{s^2}, g^{s^3}, \dots, g^{s^n}$

Prover has  $\frac{h(x)}{t(x)} = p(x)/t(x)$   $h(x) = h_0 + h_1 x + \dots + h_n x^n$

$$g^{h(s)} = g^{h_0} \cdot (g^s)^{h_1} \dots = \prod_i (g^{s^i})^{h_i}$$

Sends  $g^{\frac{u(s)}{v(s)}}, g^{\frac{v(s)}{w(s)}}, g^{\frac{w(s)}{h(s)}}, g^{h(s)}$  to verifier

$$\underline{u}(s) = \sum_i u_i(s) \cdot a_i$$

$$p(s) = \underline{u}(s) \cdot v(s) - w(s) \stackrel{?}{=} h(s) \cdot t(s)$$

Verifier checks

$$e\left(g^{\frac{u(s)}{v(s)}}, g^{v(s)}\right) / e\left(g^{\frac{w(s)}{h(s)}}, g^{h(s)}\right) \stackrel{?}{=} e\left(g^{t(s)}, g^{h(s)}\right)$$

$$e(g, g)^{\frac{u(s) \cdot v(s) - w(s)}{t(s) \cdot h(s)}} \stackrel{?}{=} e(g, g)$$

$u(s)$

Remaining problem: still need to check consistency ~~with~~ of  $g^{-1}$  etc.

Step 4) Expanding CRS to include consistency checks.

Setup  $(U, V, W)$ :  
Sampling  $\underline{\alpha}, \underline{\beta}_U, \underline{\beta}_V, \underline{\beta}_W,$

CRS :=  $g^{-1}$  for each  $i \in \mathbb{R}$

$\underline{\beta}_U, \underline{\beta}_V, \underline{\beta}_W$   $\{s^i\}, \{\alpha s^i\}, t(s), \{u_i(s)\}, \{v_i(s)\}, \{w_i(s)\}$

$g^s, (g^{\alpha})^s$  like h in pedersen

Prover  $(CRS, \bar{a})$

Computes  $p(x), h(x) = p(x)/t(x),$

$$\pi := \left( \begin{array}{cccc} g^{\underline{u}(s)} & g^{v(s)} & g^{w(s)} & g^{h(s)} \\ g^{\alpha \underline{u}(s)} & g^{\alpha v(s)} & g^{\alpha w(s)} & g^{\alpha h(s)} \\ g^{\underline{\beta}_U \cdot \underline{u}(s) + \underline{\beta}_V \cdot v(s) + \underline{\beta}_W \cdot w(s)} & & & \end{array} \right)$$

Verify: - Check  $\alpha$  and  $\beta$  terms:

$$- e(g^{\underline{u}(s)}, g^x) \stackrel{?}{=} e(g^{\alpha \underline{u}(s)}, g)$$

Same for  $v, w, h$

$$- e(g^{\underline{\beta}_U \underline{u}(s) + \dots}, g) \stackrel{?}{=} e\left(\left(\frac{\underline{\beta}_U}{g}\right), g^{\underline{u}(s)}\right) \cdot e(\dots) \cdot e(\dots)$$

$$- \text{Finally } e(g^{\underline{u}(s)}, g^{v(s)}) / e(g^{w(s)}, g) \stackrel{?}{=} e(g^{h(s)}, g^{t(s)})$$

Γ. u. . . .

What's remaining:

- how to make zero knowledge
- include consistency for statements