Pairing-Based Batch Arguments for NP with a Linear-Size CRS

Binyi Chen — Stanford University

Noel Elias — UT-Austin

David Wu — UT-Austin

Batch Arguments for NP

<u>Boolean circuit satisfiability</u>

$$\mathcal{L}_C = \{x \in \{0,1\}^n : \exists w, C(x,w) = 1\}$$

Prover

$(x_1, \ldots, x_\ell)$ →

<u>Goal:</u> convince verifier that $x_i \in \mathcal{L}_C$ for all $i \in [\ell]$

Verifier

Batch Arguments for NP

<u>Boolean circuit satisfiability</u>

$$\mathcal{L}_C = \{x \in \{0,1\}^n : \exists w, C(x,w) = 1\}$$

Prover

$$(x_1, \ldots, x_\ell) \longrightarrow$$

<u>Goal:</u> convince verifier that
$x_i \in \mathcal{L}_C$ for all $i \in [\ell]$

Verifier

<u>Proof size</u>: *Sublinear* in ℓ, i.e., $|\pi| = |C| \cdot \mathrm{poly}(\log \ell, \lambda)$

Batch Arguments for NP

Boolean circuit satisfiability

$$\mathcal{L}_C = \{x \in \{0,1\}^n : \exists w, C(x,w) = 1\}$$

Prover

$(x_1, \ldots, x_\ell)$

Goal: convince verifier that

$x_i \in \mathcal{L}_C$ for all $i \in [\ell]$

Verifier

Similar for verifier time
(beyond reading statements)

Proof size: *Sublinear* in ℓ, i.e., $|\pi| = |C| \cdot \mathrm{poly}(\log \ell, \lambda)$

Different Paths towards BARGs

SNARGs:

- iO or knowledge assumptions
- Or rely on the Random Oracle Model

Correlation Intractability:

[CJJ'21a, CJJ'21b…]

- CI-hash is a heavy machinery

Different Paths towards BARGs

SNARGs:

- iO or knowledge assumptions
- Or rely on the Random Oracle Model

Correlation Intractability:

[CJJ'21a, CJJ'21b…]

- CI-hash is a heavy machinery

Pairing-Based:

[WW'22…]

- Standard assumptions
- No heavy tool + Black box crypto

Different Paths towards BARGs

SNARGs:

- iO or knowledge assumptions
- Or rely on the Random Oracle Model

Correlation Intractability:
[CJJ'21a, CJJ'21b…]

- CI-hash is a heavy machinery

Quadratic CRS and prover-time : (

Pairing-Based:
[WW'22…]

- Standard assumptions
- No heavy tool + Black box crypto

Scalability Challenge

Quadratic CRS and prover-time : (

Pairing-Based:

[WW'22…]

- Standard assumptions
- No heavy tool + Black box crypto

Scalability Challenge

Quadratic CRS and prover-time : (

Pairing-Based: 
[WW'22…]

- Standard assumptions
- No heavy tool + Black box crypto

Example Parameters:

- CRS for $\ell = 10^5$: $> 10^8$ group elements
- Recursion? [WW'22] : Non-black-box crypto + Impractical

Q: Pairing-based BARG with linear-size CRS & quasi-linear prover time?

Our Results

A New Pairing-based BARG for NP

- CRS size: Linear in the # of instances ℓ
- Prover time: $\approx \tilde{O}_{\lambda}(|C| \cdot \ell)$
- Based on a q-type assumption

Our Results

<u>A New Pairing-based BARG for NP</u>

- CRS size: Linear in the # of instances ℓ
- Prover time: $\approx \widetilde{O}_\lambda(|C| \cdot \ell)$
- Based on a q-type assumption

Hybrid of BDH Exponent [BBG'05] +
Subgroup Decision Assumption [BGN'05]

Our Results

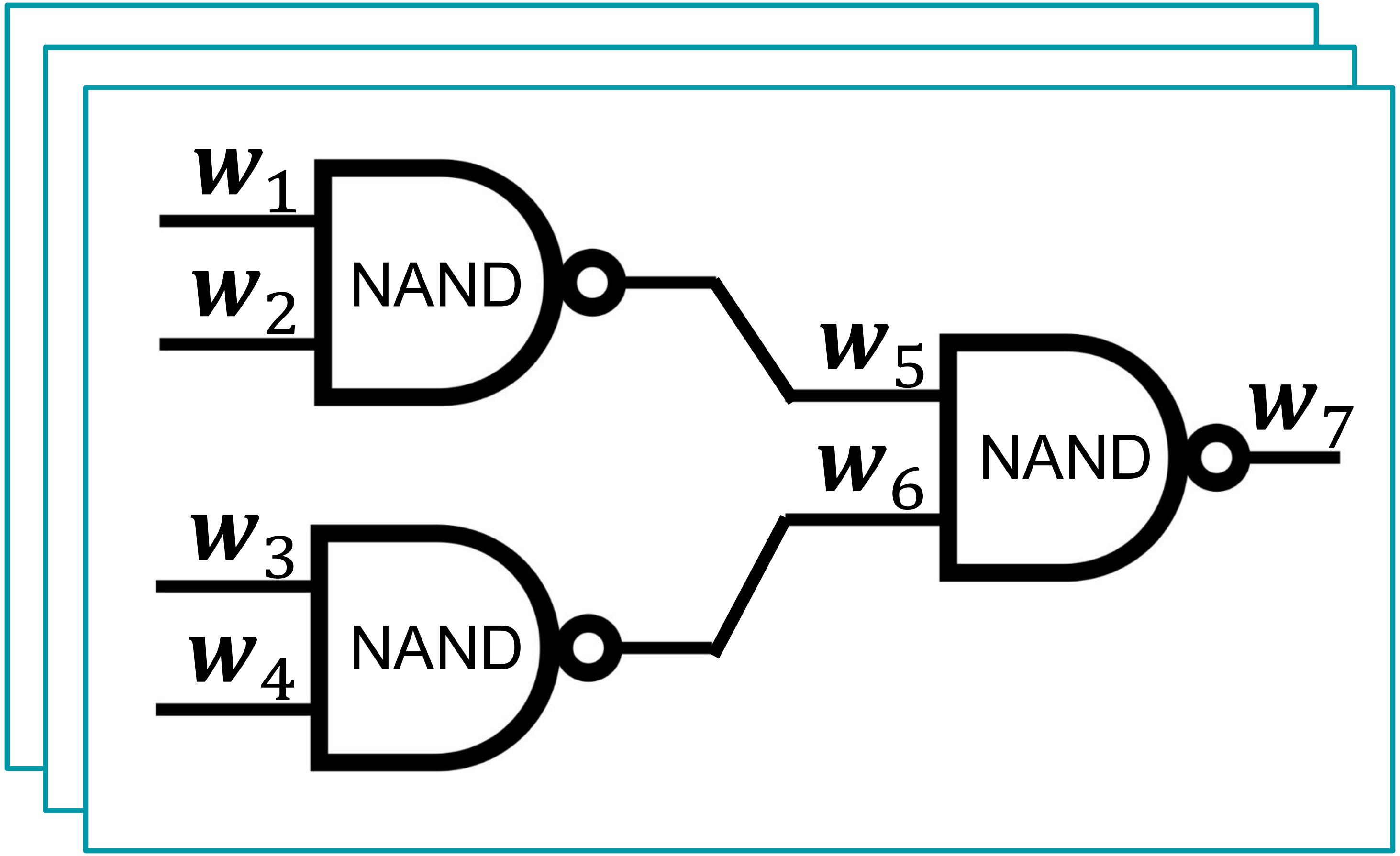
A New Pairing-based BARG for NP

- CRS size: Linear in the # of instances ℓ
- Prover time: $\approx \widetilde{O}_\lambda(|C| \cdot \ell)$
- Based on a q-type assumption

Hybrid of BDH Exponent [BBG'05] + Subgroup Decision Assumption [BGN'05]

Proven secure in the GGM

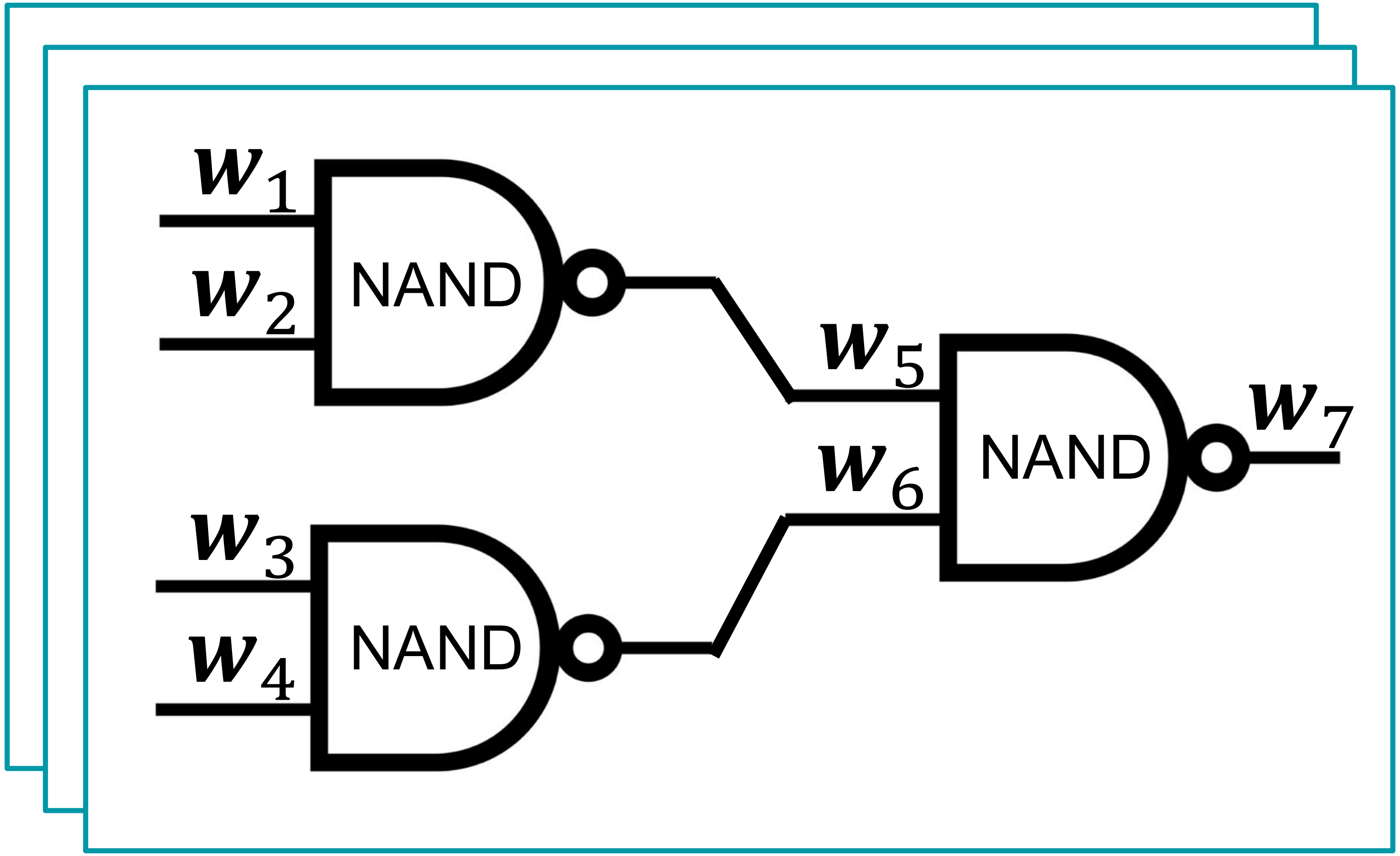
Commit-and-Prove for BARG [Waters, Wu, Crypto'22]



Vector of labels for wire i across ℓ instances

$$\boldsymbol{w}_i = (w_{i,1}, w_{i,2}, \dots, w_{i,\ell})$$

Commit-and-Prove for BARG [Waters, Wu, Crypto'22]



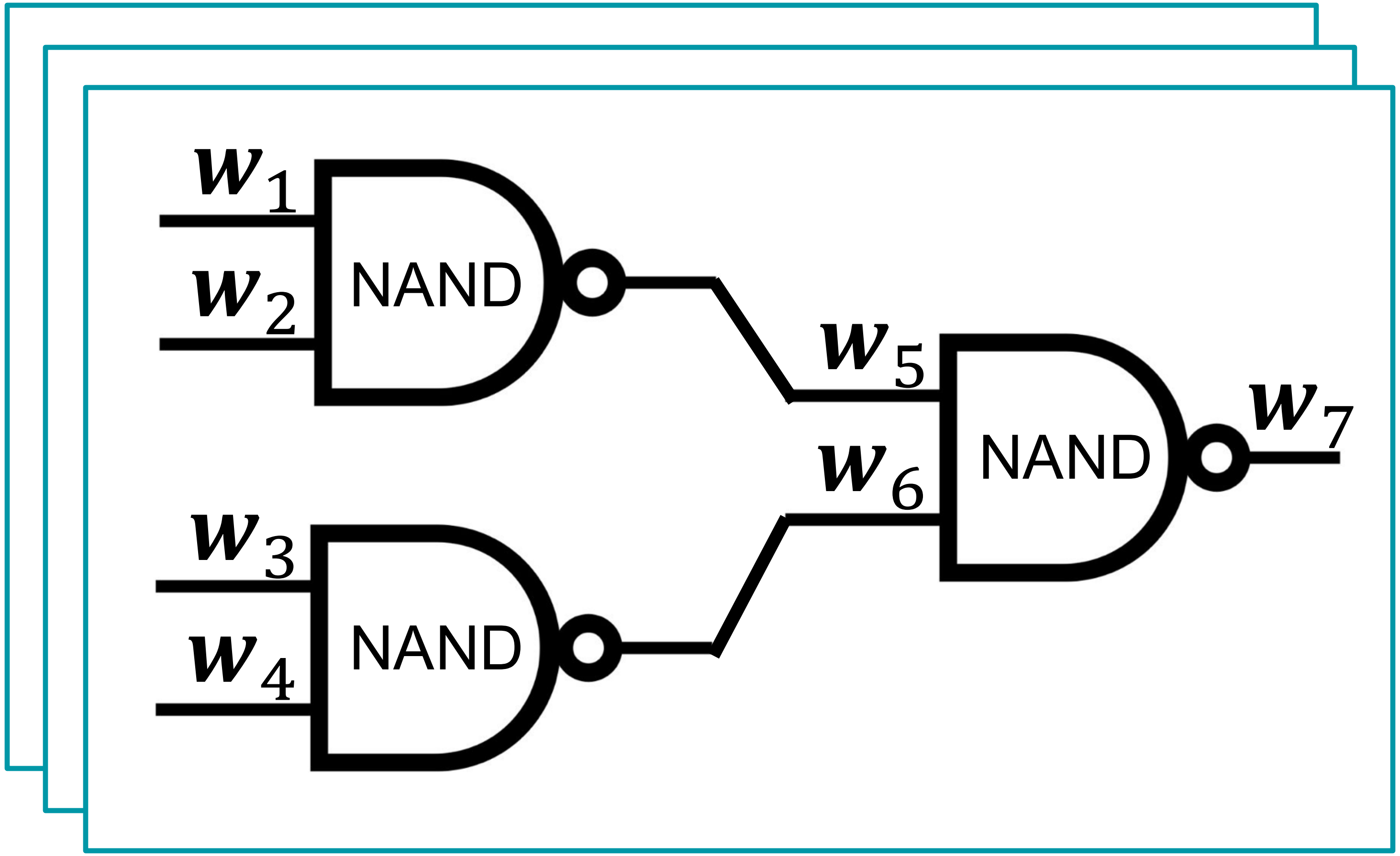
Vector of labels for wire i across ℓ instances

$$\boldsymbol{w}_i = (w_{i,1}, w_{i,2}, \dots, w_{i,\ell})$$

Pedersen comm

σ_i s.t. $|\sigma_i| = \text{poly}(\lambda)$

Commit-and-Prove for BARG [Waters, Wu, Crypto'22]



Vector of labels for wire i across ℓ instances

$$\boldsymbol{w}_i = (w_{i,1}, w_{i,2}, \dots, w_{i,\ell})$$

Pedersen comm

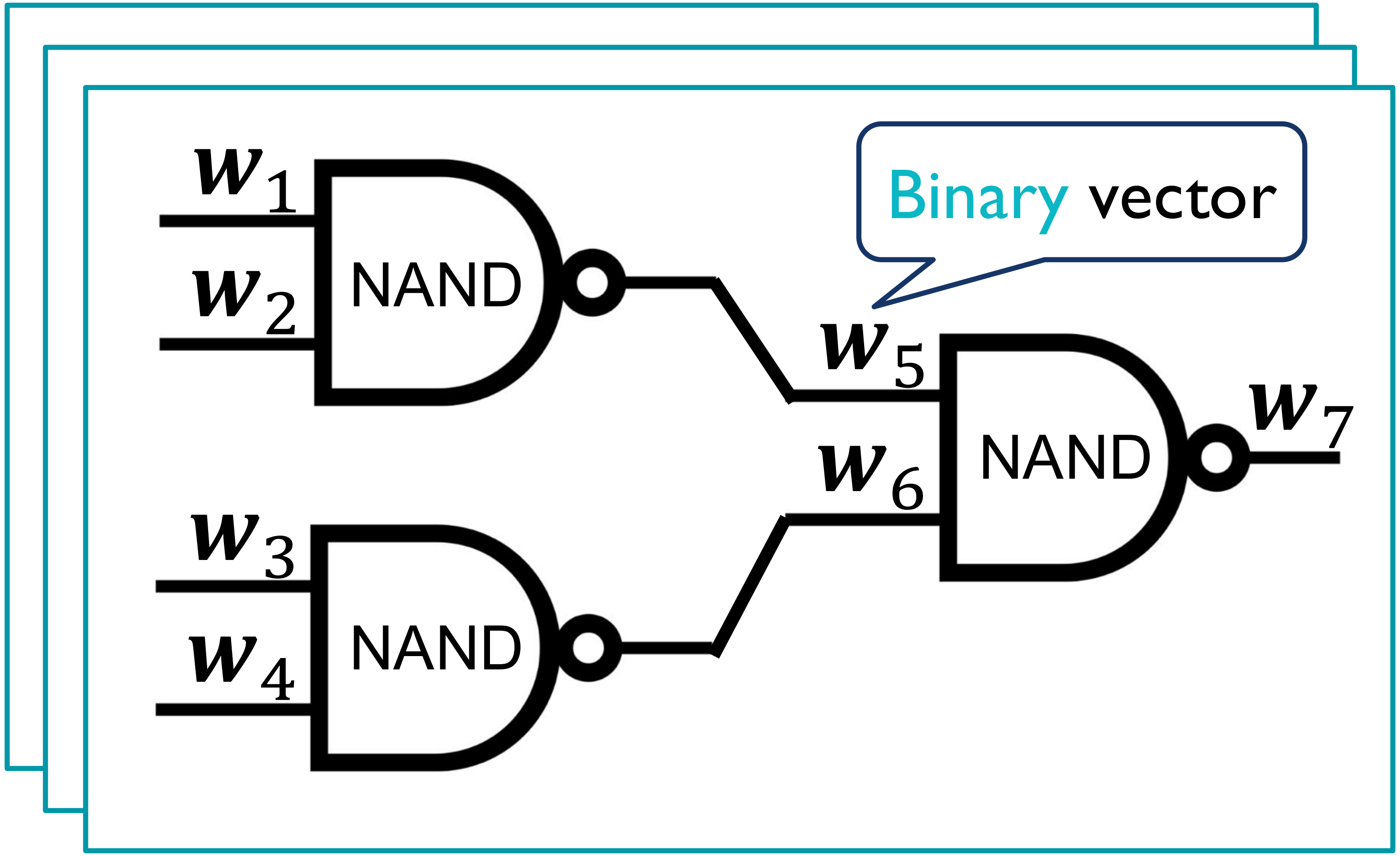
σ_i s.t. $|\sigma_i| = \mathrm{poly}(\lambda)$

Validity proofs

Wire validity

Commit-and-Prove for BARG

[Waters, Wu, Crypto'22]



Vector of labels for wire i across ℓ instances

$$\boldsymbol{w}_i = (w_{i,1}, w_{i,2}, \ldots, w_{i,\ell})$$

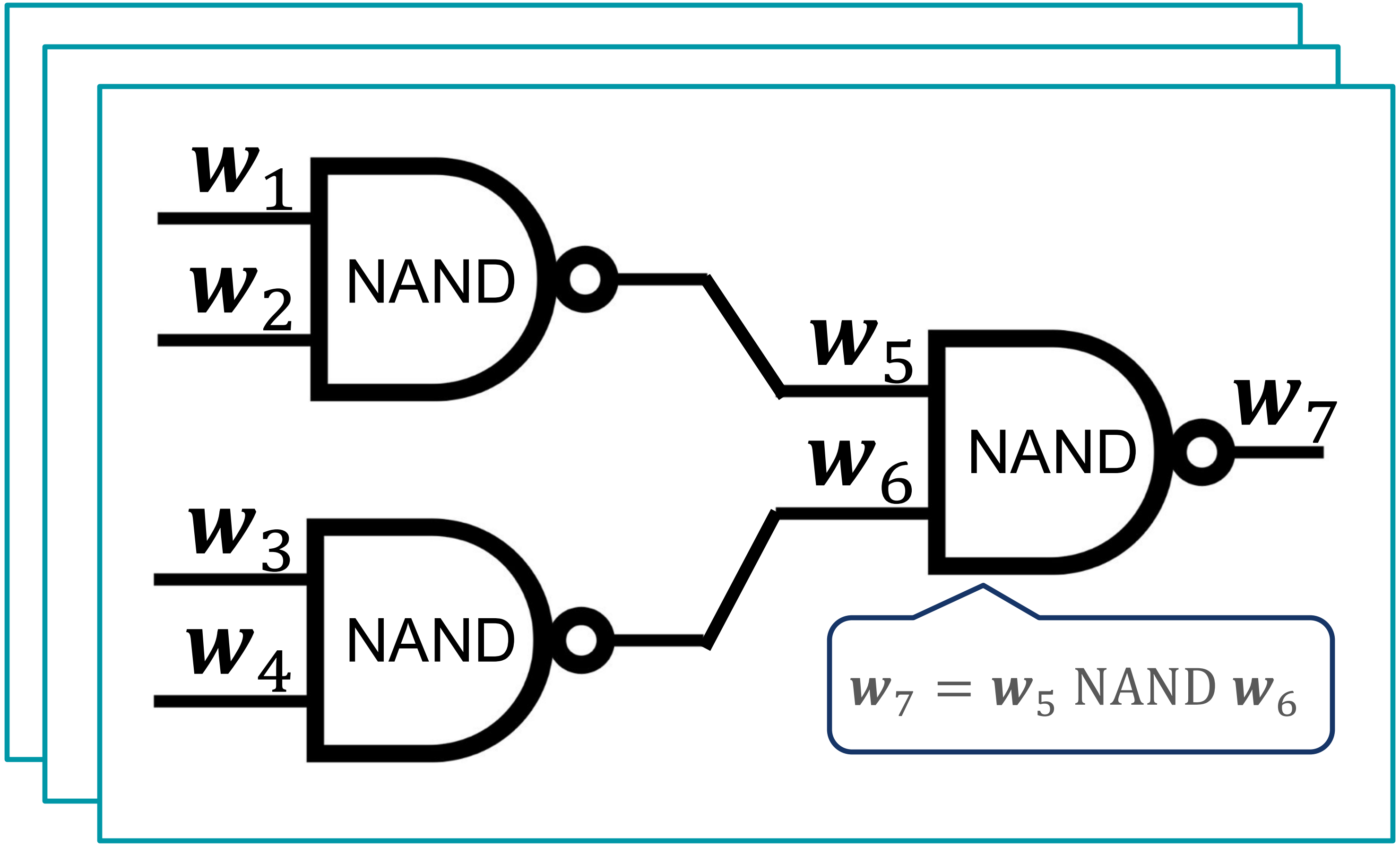
Pedersen comm

σ_i s.t. $|\sigma_i| = \mathrm{poly}(\lambda)$

Validity proofs

Wire validity

Commit-and-Prove for BARG [Waters, Wu, Crypto'22]



$\boldsymbol{w}_i = (w_{i,1}, w_{i,2}, \dots, w_{i,\ell})$

Pedersen comm

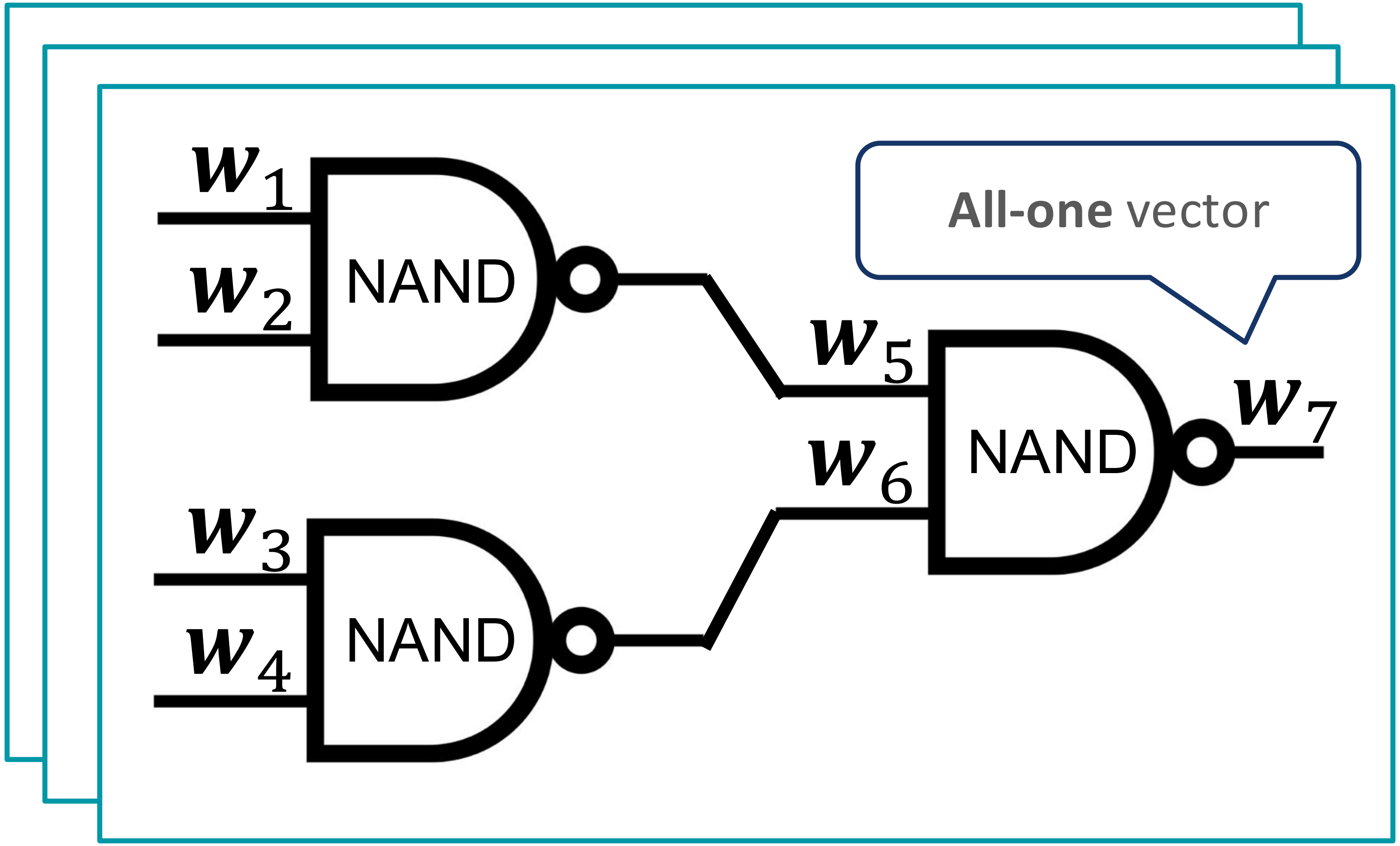
σ_i s.t. $|\sigma_i| = \mathrm{poly}(\lambda)$

Validity proofs

Gate validity

Commit-and-Prove for BARG

[Waters, Wu, Crypto'22]



$\boldsymbol{w}_i = (w_{i,1}, w_{i,2}, \dots, w_{i,\ell})$

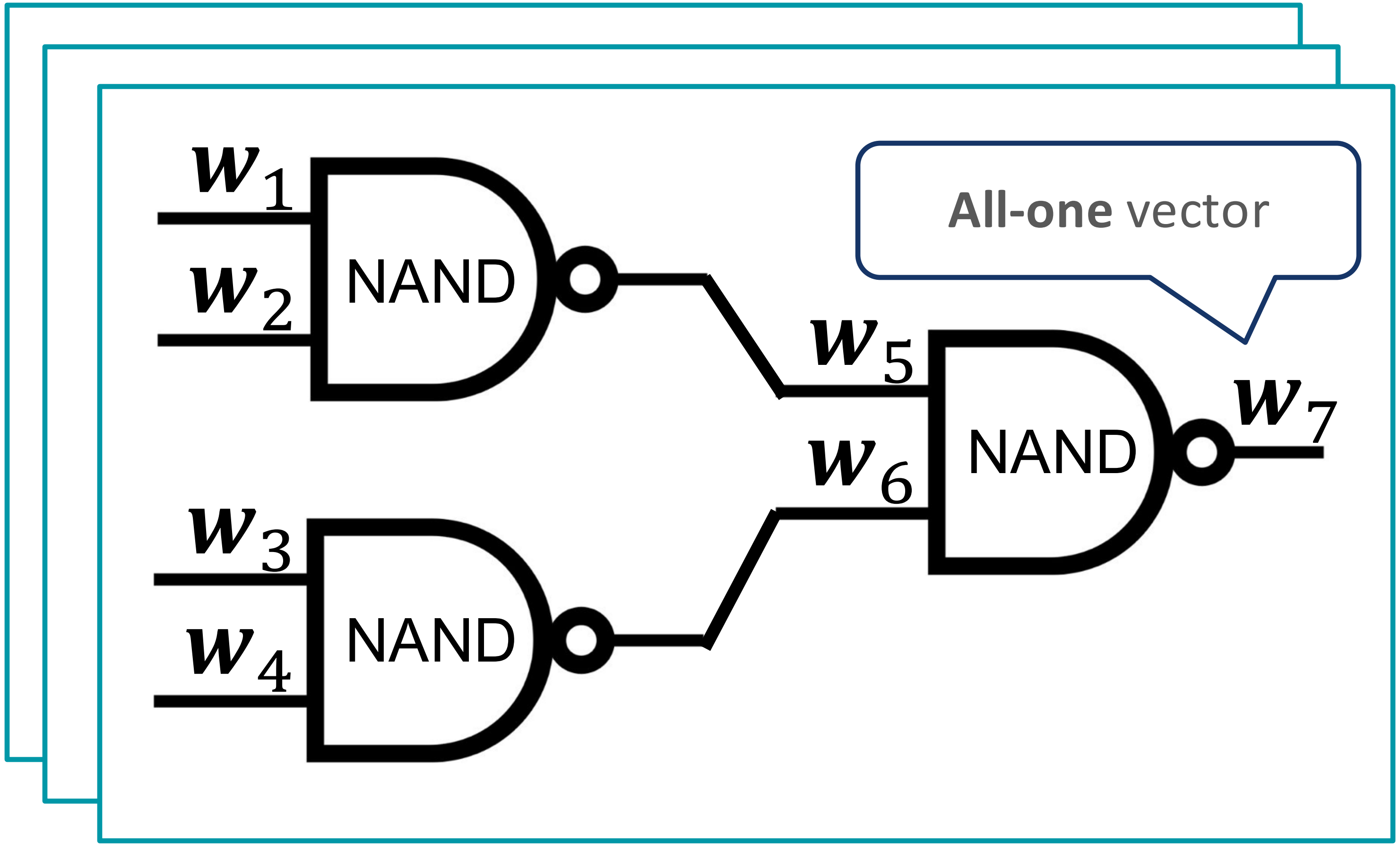
↓ Pedersen comm

σ_i s.t. $|\sigma_i| = \mathrm{poly}(\lambda)$

↓ Validity proofs

Output validity

Commit-and-Prove for BARG [Waters, Wu, Crypto'22]



$\boldsymbol{w}_i = (w_{i,1}, w_{i,2}, \dots, w_{i,\ell})$

Pedersen comm

σ_i s.t. $|\sigma_i| = \mathrm{poly}(\lambda)$

Validity proofs

Output validity

BARG proof: $\{\sigma_i\}$ + validity proofs

Q: How to compute validity proofs?

Let's focus on wire validity proofs

Quadratic Eq-Check over Exponent [WW'22]

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

Quadratic Eq-Check over Exponent [WW'22]

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

CRS: $[\alpha_1]$, $[\alpha_2]$, ... , $[\alpha_\ell]$ for rand. α_i over $\mathbb{Z}_N$

$g_p^{\alpha_\ell} \in \mathbb{G}_p$

Quadratic Eq-Check over Exponent [WW'22]

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

CRS: $[\alpha_1]$, $[\alpha_2]$, ... , $[\alpha_\ell]$ for rand. α_i over $\mathbb{Z}_N$

$g_p^{\alpha_\ell} \in \mathbb{G}_p$

Commit $\boldsymbol{x} = (x_1, \ldots, x_\ell) \in \{0,1\}^\ell$:

Quadratic Eq-Check over Exponent [WW'22]

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

CRS: $[\alpha_1]$, $[\alpha_2]$, … , $[\alpha_\ell]$ for rand. α_i over $\mathbb{Z}_N$

$g_p^{\alpha_\ell} \in \mathbb{G}_p$

Commit $\boldsymbol{x} = (x_1, \dots, x_\ell) \in \{0,1\}^\ell$:

$$\sigma_x = x_1[\alpha_1] + x_2[\alpha_2] + \cdots + x_\ell[\alpha_\ell]$$

Quadratic Eq-Check over Exponent [WW'22]

$$\sigma_x = x_1[\alpha_1] + x_2[\alpha_2] + \cdots + x_\ell[\alpha_\ell]$$

$\boldsymbol{x} = (x_1, \ldots, x_\ell)$ is binary

Quadratic Eq-Check over Exponent [WW'22]

$$\sigma_x = x_1[\alpha_1] + x_2[\alpha_2] + \cdots + x_\ell[\alpha_\ell]$$

$\boldsymbol{x} = (x_1, \dots, x_\ell)$ is binary $\Longleftrightarrow$ $x_i^2 = x_i$ for all $i \in [\ell]$

Quadratic Eq-Check over Exponent [WW'22]

$$\sigma_x = x_1[\alpha_1] + x_2[\alpha_2] + \cdots + x_\ell[\alpha_\ell]$$

$\boldsymbol{x} = (x_1, \ldots, x_\ell)$ is binary $\Longleftrightarrow$ $x_i^2 = x_i$ for all $i \in [\ell]$

$$\Longleftrightarrow \quad (x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell])^2$$

$$= (x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell]) \cdot [\alpha_1 + \cdots + \alpha_\ell]$$

$$-\left(\textstyle\sum_{i \neq j}(x_i - x_i x_j)[\alpha_i \alpha_j]\right)$$

Cross terms

Quadratic Eq-Check over Exponent [WW'22]

$$\sigma_x = x_1[\alpha_1] + x_2[\alpha_2] + \cdots + x_\ell[\alpha_\ell]$$

$\boldsymbol{x} = (x_1, \ldots, x_\ell)$ is binary $\Longleftrightarrow$ $x_i^2 = x_i$ for all $i \in [\ell]$

$$\Longleftrightarrow \quad (x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell])^2$$

$$= (x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell]) \cdot [\alpha_1 + \cdots + \alpha_\ell]$$

$$-\left(\textstyle\sum_{i \neq j}(x_i - x_i x_j)[\alpha_i \alpha_j]\right)$$

"Multiplication" = Pairing

Cross terms

Quadratic Eq-Check over Exponent [WW'22]

$$\sigma_x = x_1[\alpha_1] + x_2[\alpha_2] + \cdots + x_\ell[\alpha_\ell]$$

$\boldsymbol{x} = (x_1, \dots, x_\ell)$ is binary $\Longleftrightarrow$ $x_i^2 = x_i$ for all $i \in [\ell]$

$$\Longleftrightarrow \quad (\overbrace{x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell]}^{\sigma_x})^2$$

$$= (x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell]) \cdot [\alpha_1 + \cdots + \alpha_\ell]$$

$$-\left(\sum_{i \neq j}(x_i - x_i x_j)[\alpha_i \alpha_j]\right)$$

Cross terms

Quadratic Eq-Check over Exponent [WW'22]

$$\sigma_x = x_1[\alpha_1] + x_2[\alpha_2] + \cdots + x_\ell[\alpha_\ell]$$

$\boldsymbol{x} = (x_1, \ldots, x_\ell)$ is binary $\Longleftrightarrow$ $x_i^2 = x_i$ for all $i \in [\ell]$

$$\Longleftrightarrow \quad (\overbrace{x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell]}^{\sigma_x})^2$$

$$= (x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell]) \cdot [\alpha_1 + \cdots + \alpha_\ell]$$

$$\underbrace{-\left(\sum_{i \neq j}(x_i - x_i x_j)[\alpha_i \alpha_j]\right)}_{\text{Validity proof}}$$

Cross terms

Quadratic Eq-Check over Exponent [WW'22]

$$\sigma_x = x_1[\alpha_1] + x_2[\alpha_2] + \cdots + x_\ell[\alpha_\ell]$$

$\boldsymbol{x} = (x_1, \dots, x_\ell)$ is binary $\Longleftrightarrow$ $x_i^2 = x_i$ for all $i \in [\ell]$

$$\Longleftrightarrow \quad (\overbrace{x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell]}^{\sigma_x})^2$$

$$= (x_1[\alpha_1] + \cdots + x_\ell[\alpha_\ell]) \cdot [\alpha_1 + \cdots + \alpha_\ell]$$

$$\underbrace{-\left(\sum_{i \neq j}(x_i - x_i x_j)[\alpha_i \alpha_j]\right)}_{\text{Validity proof}}$$

Cross terms

Caveat: CRS includes $\{[\alpha_i \alpha_j]\}_{i \neq j}$

ℓ^2-size

Q: Check quadratic equations without cross-terms?

Q: Check quadratic equations without cross-terms?

Idea: Vector commitment

Polynomial commitment

Quadratic Check using Polynomials

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

Quadratic Check using Polynomials

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

CRS: $[1]$, $[\alpha]$, … , $[\alpha^\ell]$ for rand. α over $\mathbb{Z}_N$

Quadratic Check using Polynomials

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

CRS: $[1]$, $[\alpha]$, ... , $[\alpha^\ell]$ for rand. α over $\mathbb{Z}_N$

Commit $\boldsymbol{w} = (w_1, \ldots, w_\ell) \in \{0,1\}^\ell$:

Quadratic Check using Polynomials

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

CRS: $[1]$, $[\alpha]$, ... , $[\alpha^\ell]$ for rand. α over $\mathbb{Z}_N$

Commit $\boldsymbol{w} = (w_1, \dots, w_\ell) \in \{0,1\}^\ell$:

$$\boldsymbol{w} \xrightarrow{\text{Interpolate}} \phi(x) \text{ s.t.}$$

$\phi(i) = w_i$ for all $i \in [\ell]$

Quadratic Check using Polynomials

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

CRS: $[1]$, $[\alpha]$, … , $[\alpha^\ell]$ for rand. α over $\mathbb{Z}_N$

Commit $\boldsymbol{w} = (w_1, \dots, w_\ell) \in \{0,1\}^\ell$:

$$\boldsymbol{w} \xrightarrow{\text{Interpolate}} \phi(x) \text{ s.t. } \phi(i) = w_i \text{ for all } i \in [\ell] \xrightarrow{\text{Commit}} \sigma_{\boldsymbol{w}} = [\phi(\alpha)]$$

Quadratic Check using Polynomials

$\mathbb{G}$: Group of order $N = pq$

$\mathbb{G}_p$: Subgroup of order p w/ generator g_p

CRS: $[1]$, $[\alpha]$, … , $[\alpha^\ell]$ for rand. α over $\mathbb{Z}_N$

Commit $\boldsymbol{w} = (w_1, \dots, w_\ell) \in \{0,1\}^\ell$:

Compute from CRS and coefficients of ϕ

$\boldsymbol{w} \xrightarrow{\text{Interpolate}} \phi(x)$ s.t. $\phi(i) = w_i$ for all $i \in [\ell]$ $\xrightarrow{\text{Commit}} \sigma_{\boldsymbol{w}} = [\phi(\alpha)]$

Quotient Check for Quadratic Equations

Commitment: $\sigma_{\boldsymbol{w}} = [\phi(\alpha)]$

$\boldsymbol{w} = (w_1, \ldots, w_\ell)$ is binary $\Longleftrightarrow$ $w_i^2 = w_i$ for all $i \in [\ell]$

Quotient Check for Quadratic Equations

Commitment: $\sigma_{\boldsymbol{w}} = [\phi(\alpha)]$

$\boldsymbol{w} = (w_1, \dots, w_\ell)$ is binary $\Longleftrightarrow$ $w_i^2 = w_i$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi(i)^2 = \phi(i)$ for all $i \in [\ell]$

Quotient Check for Quadratic Equations

Commitment: $\sigma_{\boldsymbol{w}} = [\phi(\alpha)]$

$\boldsymbol{w} = (w_1, \ldots, w_\ell)$ is binary $\Longleftrightarrow$ $w_i^2 = w_i$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi(i)^2 = \phi(i)$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi^2 - \phi = Z_\ell(x) \cdot Q(x)$

Quotient Check for Quadratic Equations

Commitment: $\sigma_{\boldsymbol{w}} = [\phi(\alpha)]$

$\boldsymbol{w} = (w_1, \dots, w_\ell)$ is binary $\Longleftrightarrow$ $w_i^2 = w_i$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi(i)^2 = \phi(i)$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi^2 - \phi = Z_\ell(x) \cdot Q(x)$

- $Z_\ell(x) = \prod_{i \in [\ell]}(x - i)$
- $Q(x)$: quotient polynomial

Quotient Check for Quadratic Equations

Commitment: $\sigma_{\boldsymbol{w}} = [\phi(\alpha)]$

$\boldsymbol{w} = (w_1, \dots, w_\ell)$ is binary $\Longleftrightarrow$ $w_i^2 = w_i$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi(i)^2 = \phi(i)$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi^2 - \phi = Z_\ell(x) \cdot Q(x)$

- $Z_\ell(x) = \prod_{i \in [\ell]} (x - i)$
- $Q(x)$: quotient polynomial

$\overset{\approx}{\Longleftrightarrow}$ $[\phi(\alpha)] \cdot [\phi(\alpha)] - [\phi(\alpha)] \cdot [1] = [Z_\ell(\alpha)] \cdot [Q(\alpha)]$

Quotient Check for Quadratic Equations

<u>Commitment:</u> $\sigma_{\boldsymbol{w}} = [\phi(\alpha)]$

$\boldsymbol{w} = (w_1, \dots, w_\ell)$ is binary $\Longleftrightarrow$ $w_i^2 = w_i$ for all $i \in [\ell]$

$\Longleftrightarrow \quad \phi(i)^2 = \phi(i)$ for all $i \in [\ell]$

$\Longleftrightarrow \quad \phi^2 - \phi = Z_\ell(x) \cdot Q(x)$

- $Z_\ell(x) = \prod_{i\in[\ell]}(x - i)$
- $Q(x)$: quotient polynomial

$\overset{\approx}{\Longleftrightarrow} \quad [\phi(\alpha)] \cdot [\phi(\alpha)] - [\phi(\alpha)] \cdot [1] = [Z_\ell(\alpha)] \cdot [Q(\alpha)]$

"Multiplication" = Pairing

Quotient Check for Quadratic Equations

<u>Commitment:</u> $\sigma_{\boldsymbol{w}} = [\phi(\alpha)]$

$\boldsymbol{w} = (w_1, \ldots, w_\ell)$ is binary $\Longleftrightarrow$ $w_i^2 = w_i$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi(i)^2 = \phi(i)$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi^2 - \phi = Z_\ell(x) \cdot Q(x)$

- $Z_\ell(x) = \prod_{i \in [\ell]}(x - i)$
- $Q(x)$: quotient polynomial

$$\overset{\approx}{\Longleftrightarrow} \quad [\phi(\alpha)] \cdot [\phi(\alpha)] - [\phi(\alpha)] \cdot [1] = [Z_\ell(\alpha)] \cdot \underbrace{[Q(\alpha)]}_{\text{Validity proof}}$$

"Multiplication" = Pairing

Quotient Check for Quadratic Equations

Commitment: $\sigma_{\boldsymbol{w}} = [\phi(\alpha)]$

- Linear CRS size
- $O(\ell \log \ell)$ $\mathbb{Z}_N$-ops + $O(\ell)$ $\mathbb{G}$-ops

Interpolation set = Roots-of-unity

$\boldsymbol{w} = (w_1, \ldots, w_\ell)$ is binary $\Longleftrightarrow$ $w_i^2 = w_i$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi(i)^2 = \phi(i)$ for all $i \in [\ell]$

$\Longleftrightarrow$ $\phi^2 - \phi = Z_\ell(x) \cdot Q(x)$

- $Z_\ell(x) = \prod_{i \in [\ell]} (x - i)$
- $Q(x)$: quotient polynomial

$\overset{\approx}{\Longleftrightarrow}$ $[\phi(\alpha)] \cdot [\phi(\alpha)] - [\phi(\alpha)] \cdot [1] = [Z_\ell(\alpha)] \cdot \underbrace{[Q(\alpha)]}_{\text{Validity proof}}$

"Multiplication" = Pairing

Q: How about other validity proofs?

Similar approach, as relations are quadratic

Comparison with [KZG'10]

[KZG'10]:

- Knowledge soundness
- Knowledge assumptions or AGM

Our result:

- Somewhere extractability
- Security in the standard model
- Falsifiable assumption

Comparison with [KZG'10]

[KZG'10]:

- Knowledge soundness
- Knowledge assumptions or AGM

Our result:

- Somewhere extractability
- Security in the standard model
- Falsifiable assumption

Somewhere Extractability [Choudhuri, Jain, Jin'21]

Trapdoor CRS Generation:

$i^* \in [\ell] \longrightarrow \boxed{\text{TrapGen}}$

Somewhere Extractability [Choudhuri, Jain, Jin'21]

Trapdoor CRS Generation:

$$i^* \in [\ell] \longrightarrow \boxed{\text{TrapGen}} \longrightarrow \boxed{\mathrm{CRS}^*} + \boxed{\mathrm{td}^*}$$

Somewhere Extractability [Choudhuri, Jain, Jin'21]

<u>Trapdoor CRS Generation:</u>

Normal $\boxed{\mathrm{CRS}}$

$$\approx_c$$

$$i^* \in [\ell] \longrightarrow \boxed{\text{TrapGen}} \longrightarrow \boxed{\mathrm{CRS}^*} + \boxed{\mathrm{td}^*}$$

Somewhere Extractability [Choudhuri, Jain, Jin'21]

Trapdoor CRS Generation:

Normal $\boxed{\text{CRS}}$

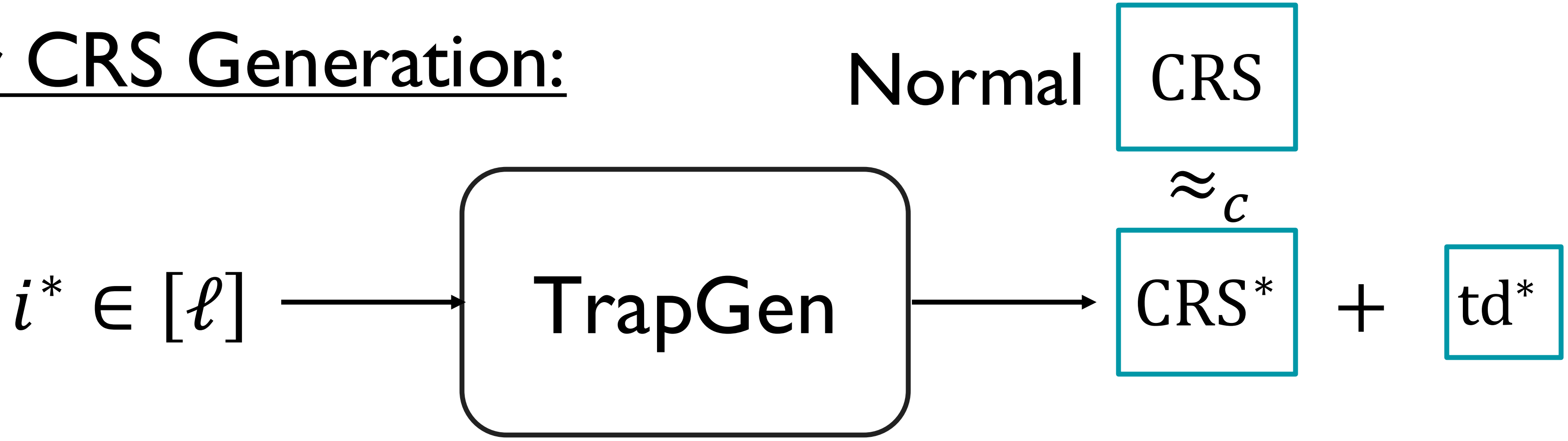
$\approx_c$

$$i^* \in [\ell] \longrightarrow \boxed{\text{TrapGen}} \longrightarrow \boxed{\text{CRS}^*} + \boxed{\text{td}^*}$$

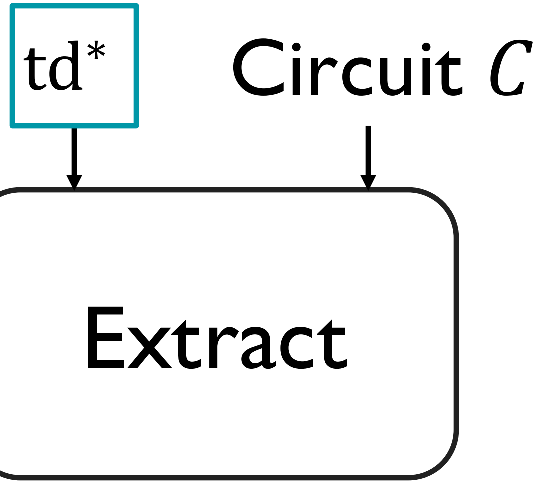
Somewhere Extraction:

Somewhere Extractability [Choudhuri, Jain, Jin'21]

Trapdoor CRS Generation:

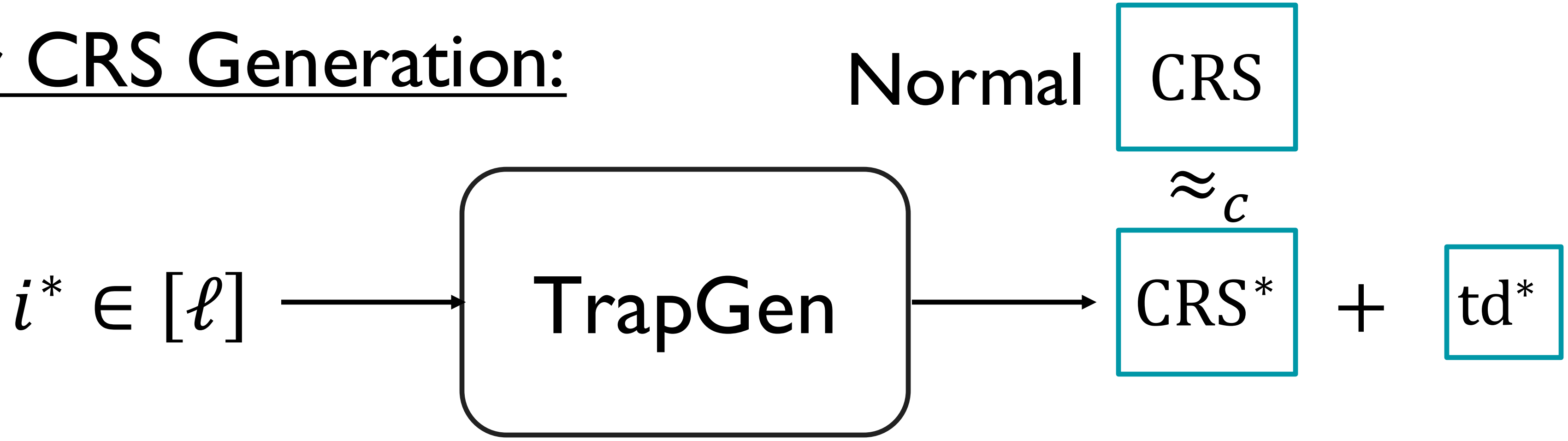


Somewhere Extraction:

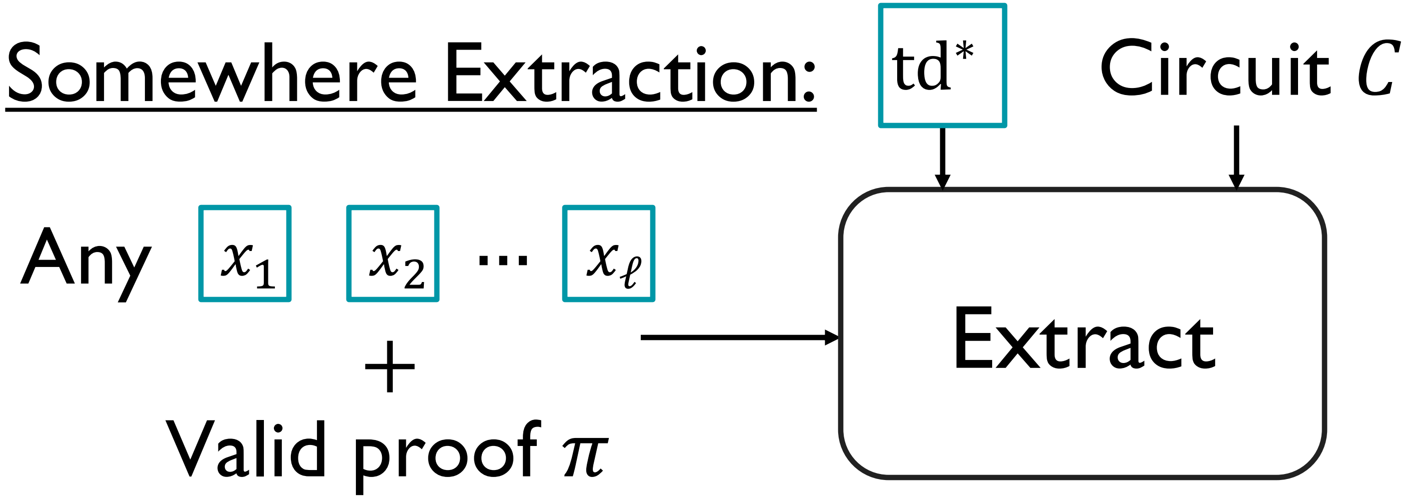


Somewhere Extractability [Choudhuri, Jain, Jin'21]

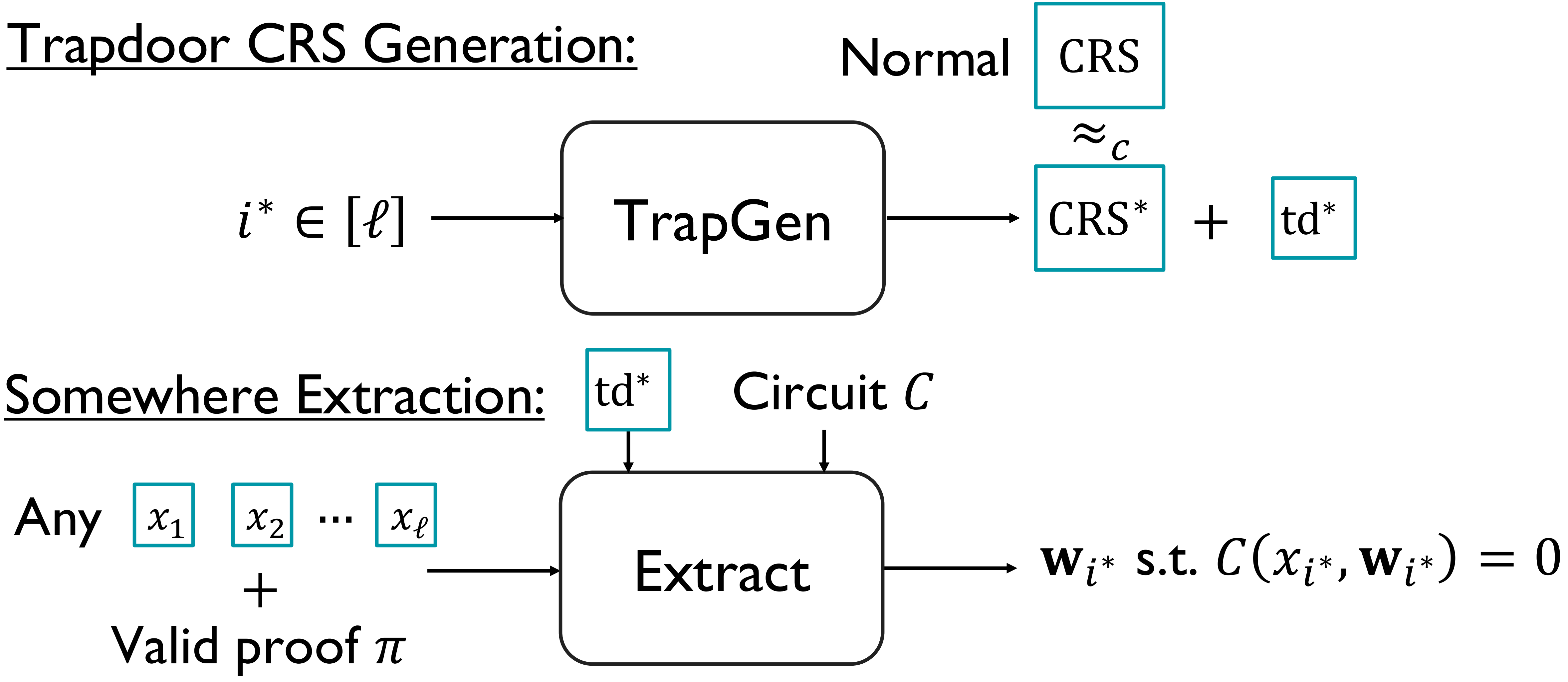
Trapdoor CRS Generation:



Somewhere Extraction:



Somewhere Extractability [Choudhuri, Jain, Jin’21]



CRS Indistinguishability

Trapdoor CRS Generation: $i^* \in [\ell]$:

CRS Indistinguishability

Trapdoor CRS Generation: $i^* \in [\ell]$:

$\boxed{\mathrm{td}^*} = g_q \in \mathbb{G}_q$

CRS Indistinguishability

Trapdoor CRS Generation: $i^* \in [\ell]$: $g_p^{\alpha^\ell} g_q^{{i^*}^\ell}$

$$\boxed{\mathrm{CRS}^*} = [1]\cdot[1], [\alpha]\cdot[i^*], \ldots, [\alpha^\ell]\cdot[{i^*}^\ell]$$

$$\boxed{\mathrm{td}^*} = g_q \in \mathbb{G}_q$$

CRS Indistinguishability

<u>Trapdoor CRS Generation:</u> $i^* \in [\ell]$:

$g_p^{\alpha^\ell} g_q^{i*^\ell}$

$$\boxed{\mathrm{CRS}^*} = [1] \cdot [1], [\alpha] \cdot [i^*], \ldots, [\alpha^\ell] \cdot [i^{*\ell}]$$

$$\approx_c$$

$$\boxed{\mathrm{CRS}} = [1], [\alpha], \ldots, [\alpha^\ell]$$

$$\boxed{\mathrm{td}^*} = g_q \in \mathbb{G}_q$$

CRS Indistinguishability

Trapdoor CRS Generation: $i^* \in [\ell]$: $g_p^{\alpha^\ell} g_q^{i*^\ell}$

$\boxed{\mathrm{CRS}^*} = [1] \cdot [1], [\alpha] \cdot [i^*], \dots, [\alpha^\ell] \cdot [i^{*\ell}]$

$\approx_c$

$\boxed{\mathrm{CRS}} = [1], \quad [\alpha] \quad , \dots, [\alpha^\ell]$

Subgroup Decision Exponent Assumption:
$[\alpha], \dots, [\alpha^\ell], g_p$
$\approx_c [\alpha], \dots, [\alpha^\ell], g_p g_q$

$\boxed{\mathrm{td}^*} = g_q \in \mathbb{G}_q$

CRS Indistinguishability

Trapdoor CRS Generation: $i^* \in [\ell]$:

$g_p^{\alpha^\ell} g_q^{i*^\ell}$

True in GGM

$\boxed{\mathrm{CRS}^*} = [1]\cdot[1], [\alpha]\cdot[i^*], \ldots, [\alpha^\ell]\cdot[i^{*\ell}]$

$\approx_c$

$\boxed{\mathrm{CRS}} = [1], [\alpha], \ldots, [\alpha^\ell]$

Subgroup Decision Exponent Assumption:

$[\alpha], \ldots, [\alpha^\ell], g_p$

$\approx_c [\alpha], \ldots, [\alpha^\ell], g_p g_q$

$\boxed{\mathrm{td}^*} = g_q \in \mathbb{G}_q$

Somewhere Extraction

$\boxed{\mathrm{CRS}^*} = [1] \cdot [1], [\alpha] \cdot [i^*], \ldots, [\alpha^\ell] \cdot [{i^*}^\ell]$

$\boxed{\mathrm{td}^*} = g_q :$

Somewhere Extraction

$\boxed{\mathrm{CRS}^*} = [1] \cdot [1], [\alpha] \cdot [i^*], \ldots, [\alpha^\ell] \cdot [i^{*\ell}]$

A valid wire commitment from the prover is of the form:

$$\sigma_{\boldsymbol{w}} = [\phi(\alpha)] \cdot [\phi(i^*)] = [\phi(\alpha)] \cdot [w_{i^*}]$$

$\boxed{\mathrm{td}^*} = g_q :$

Somewhere Extraction

$\boxed{\mathrm{CRS}^*} = [1] \cdot [1], [\alpha] \cdot [i^*], \ldots, [\alpha^\ell] \cdot [{i^*}^\ell]$

A valid wire commitment from the prover is of the form:

$\sigma_{\boldsymbol{w}} = [\phi(\alpha)] \cdot [\phi(i^*)] = [\phi(\alpha)] \cdot [w_{i^*}]$

Use td^* to project $\sigma_{\boldsymbol{w}}$ onto subgroup $\mathbb{G}_q$

$\boxed{\mathrm{td}^*} = g_q$:

Somewhere Extraction

$\boxed{\mathrm{CRS}^*} = [1] \cdot [1], [\alpha] \cdot [i^*], \ldots, [\alpha^\ell] \cdot [{i^*}^\ell]$

A valid wire commitment from the prover is of the form:

$$\sigma_{\boldsymbol{w}} = [\phi(\alpha)] \cdot [\phi(i^*)] = [\phi(\alpha)] \cdot [w_{i^*}]$$

Use td^* to project $\sigma_{\boldsymbol{w}}$ onto subgroup $\mathbb{G}_q$

$\boxed{\mathrm{td}^*} = g_q$: $\quad e(g_q, [\phi(\alpha)] \cdot [w_{i^*}]) = e(g_q, g_q)^{w_{i^*}}$

Somewhere Extraction

$\boxed{\mathrm{CRS}^*} = [1] \cdot [1], [\alpha] \cdot [i^*], \ldots, [\alpha^\ell] \cdot [{i^*}^\ell]$

A valid wire commitment from the prover is of the form:

$$\sigma_{\boldsymbol{w}} = [\phi(\alpha)] \cdot [\phi(i^*)] = [\phi(\alpha)] \cdot [w_{i^*}]$$

Use td^* to project $\sigma_{\boldsymbol{w}}$ onto subgroup $\mathbb{G}_q$

Allow extraction of $w_{i^*} \in \{0, 1\}$

$\boxed{\mathrm{td}^*} = g_q$: $\quad e\left(g_q, [\phi(\alpha)] \cdot [w_{i^*}]\right) = e\left(g_q, g_q\right)^{w_{i^*}}$

Summary

- Extend [WW'22] to the polynomial setting
- Linear-size CRS, quasilinear prover time, black-box crypto
- Security from falsifiable assumptions

Open Problems:

Extend to prime-order groups?

Lattice-based constructions?

THANK YOU

Eprint 2025/1323