Caulk: Lookup Arguments in Sublinear Time

Arantxa Zapico
Universitat Pompeu Fabra

Vitalik Buterin
Dmitry Khovratovich
Mary Maller
Mark Simkin
Ethereum Foundation

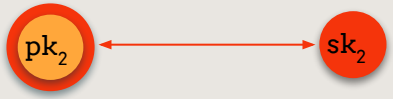
Anca Nitulescu
Protocol Labs

MOTIVATION

MEMBERSHIP PROOFS

MEMBERSHIP PROOFS

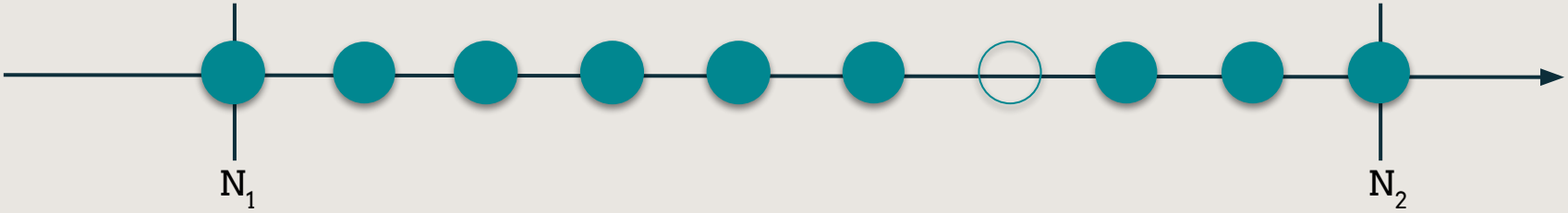
MEMBERSHIP PROOFS



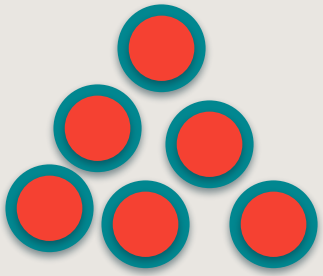
RANGE PROOFS

RANGE PROOFS

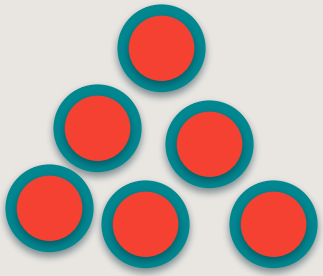
RANGE PROOFS



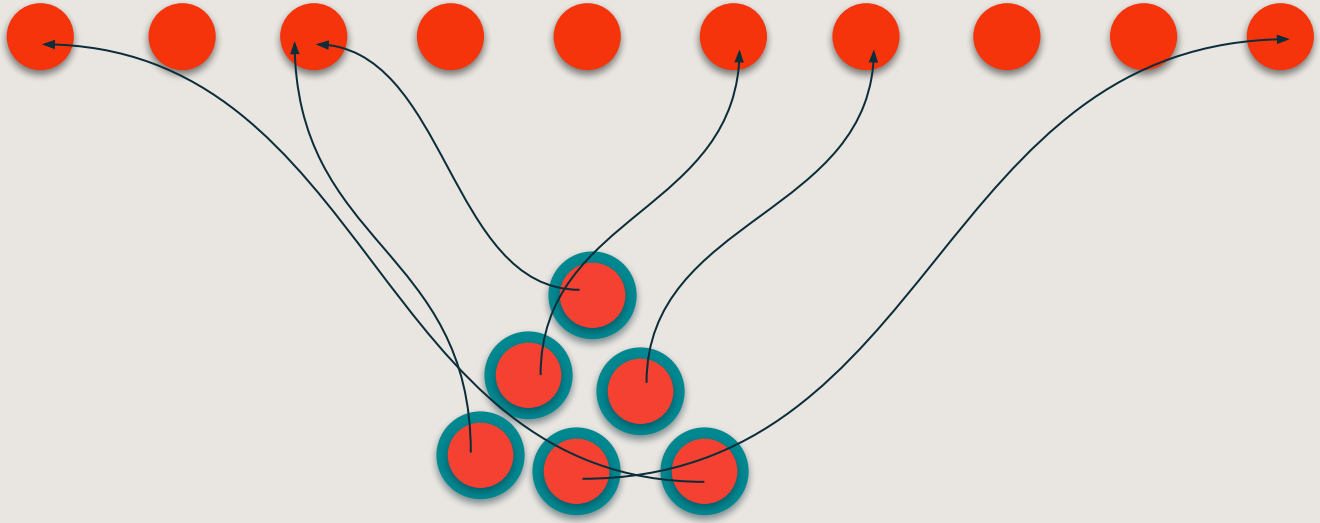
LOOKUP TABLES



LOOKUP TABLES



LOOKUP TABLES



STATE OF THE ART

STATE OF THE ART

Discrete-log

STATE OF THE ART

Discrete-log

- Transparent setup
- Linear prover and verifier

STATE OF THE ART

Discrete-log

- Transparent setup
- Linear prover and verifier

RSA Accumulators

STATE OF THE ART

Discrete-log

- Transparent setup
- Linear prover and verifier

RSA Accumulators

- Constant prover
- Trusted parameters

STATE OF THE ART

Discrete-log

- Transparent setup
- Linear prover and verifier

Merkle Trees

RSA Accumulators

- Constant prover
- Trusted parameters

STATE OF THE ART

Discrete-log

- Transparent setup
- Linear prover and verifier

Merkle Trees

- Transparent setup
- Need a zkSNARK on top

RSA Accumulators

- Constant prover
- Trusted parameters

STATE OF THE ART

Discrete-log

- Transparent setup
- Linear prover and verifier

Merkle Trees

- Transparent setup
- Need a zkSNARK on top

RSA Accumulators

- Constant prover
- Trusted parameters

Pairing-based

STATE OF THE ART

Discrete-log

- Transparent setup
- Linear prover and verifier

Merkle Trees

- Transparent setup
- Need a zkSNARK on top

RSA Accumulators

- Constant prover
- Trusted parameters

Pairing-based

- Constant proof + verifier
- Linear prover

CAULK

Pairing-based

CAULK

Pairing-based

Logaritmic prover + constant proof

log(log) verifier

DEFINITION

DEFINITION

DEFINITION

Position-hiding linkability for two VC schemes

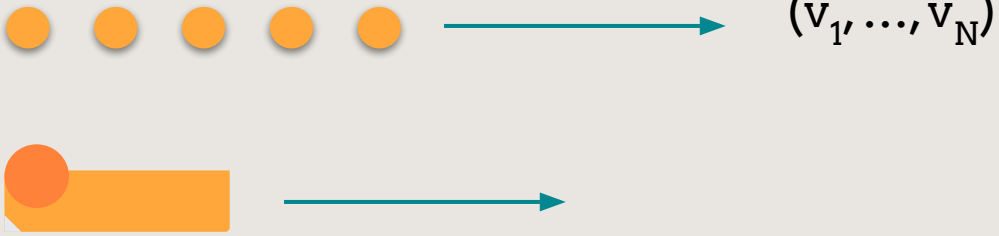
Everything in 

is also in 

KZG

KZG

KZG



KZG

$(v_1, \ldots, v_N)$

$H=\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}, \quad \omega^N=1$

KZG

$(v_1, \ldots, v_N)$

$H=\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}, \quad \omega^N=1$

$\{\lambda_i(X)\}$, $\lambda_i(\omega^{i-1})=1$, $\lambda_i(\omega^j)=0$

KZG

$(v_1, \ldots, v_N)$

$H=\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}, \quad \omega^N=1$

$\{\lambda_i(X)\}$, $\lambda_i(\omega^{i-1})=1$, $\lambda_i(\omega^j)=0$

$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$

KZG

$(v_1, \ldots, v_N)$

$H=\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}, \quad \omega^N=1$

$\{\lambda_i(X)\}$, $\lambda_i(\omega^{i-1})=1$, $\lambda_i(\omega^j)=0$

$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$

$C(\omega^{i-1})=v_i$

ROOTS OF UNITY

$$H=\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}, \qquad \omega^N=1$$

ROOTS OF UNITY

$H=\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}, \quad \omega^N=1$

1. Sparse Lagrange and vanishing polynomials

ROOTS OF UNITY

$H=\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}, \quad \omega^N=1$

1. Sparse Lagrange and vanishing polynomials

$z_H(X)=X^N-1 \qquad \lambda_i(X)=(\omega^{i-1}(X^N-1))((X-\omega^{i-1})N)^{-1}$

ROOTS OF UNITY

$H=\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}, \quad \omega^N=1$

1. Sparse Lagrange and vanishing polynomials

$z_H(X)=X^N-1 \qquad \lambda_i(X)=(\omega^{i-1}(X^N-1))((X-\omega^{i-1})N)^{-1}$

2. Any u such that $u^N=1$ is an Nth root of unity

ROOTS OF UNITY

$$H=\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}, \quad \omega^N=1$$

1. Sparse Lagrange and vanishing polynomials

$$z_H(X)=X^N-1 \qquad \lambda_i(X)=(\omega^{i-1}(X^N-1))((X-\omega^{i-1})N)^{-1}$$

2. Any u such that $u^N=1$ is an Nth root of unity

If $u^N=1 \longrightarrow u=\omega^{something}$

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

KZG + TABDFK

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

- Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

Verifier checks

$$e([C(x)],[v_i])=e([(x-\omega^{i-1})],[Q_i(x)])$$

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

Verifier checks

$$e([C(x)],[v_i])=e([(x-\omega^{i-1})],[Q_i(x)])$$

KZG + TABDFK

$$C(X)=\Sigma_i v_i \lambda_i(X)$$

Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

Verifier checks

$$e([C(x)],[v_i])=e([(x-\omega^{i-1})],[Q_i(x)])$$

Prover sends $[C_I(x)]$, $[\Pi_{i\varepsilon I}(x-\omega^{i-1})]$, $[Q_I(x)]$ s.t:

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

Verifier checks

$$e([C(x)],[v_i])=e([(x-\omega^{i-1})],[Q_i(x)])$$

Prover sends $[C_I(x)]$, $[\Pi_{i\varepsilon I}(x-\omega^{i-1})]$, $[Q_I(x)]$ s.t:

$$C_I(X)=\Sigma_{i\varepsilon I} v_i\, \tau_i(X)$$

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

Verifier checks

$$e([C(x)],[v_i])=e([(x-\omega^{i-1})],[Q_i(x)])$$

Prover sends $[C_I(x)]$, $[\Pi_{i\varepsilon\, I}(x-\omega^{i-1})]$, $[Q_I(x)]$ s.t:

$$C_I(X)=\Sigma_{i\varepsilon\, I} v_i\, \tau_i(X)$$

$$H_I=\{\omega^{i-1}\}_{i\varepsilon\, I}$$

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

Verifier checks

$$e([C(x)],[v_i])=e([(x-\omega^{i-1})],[Q_i(x)])$$

Prover sends $[C_I(x)]$, $[\Pi_{i\varepsilon\, I}(x-\omega^{i-1})]$, $[Q_I(x)]$ s.t:

$$C(X)-C_I(X)=\Pi_{i\varepsilon\, I}\,(X-\omega^{i-1})\,Q_I(X)$$

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

Verifier checks

$$e([C(x)],[v_i])=e([(x-\omega^{i-1})],[Q_i(x)])$$

Prover sends $[C_I(x)]$, $[\Pi_{i\varepsilon I}(x-\omega^{i-1})]$, $[Q_I(x)]$ s.t:

$$C(X)-C_I(X)=\Pi_{i\varepsilon I}\,(X-\omega^{i-1})\,Q_I(X)$$

Verifier checks

$$e([C(x)],\,[C_I(x)])=e([\Pi_{i\varepsilon I}(x-\omega^{i-1})],[Q_I(x)])$$

KZG + TABDFK

$$C(X)=\Sigma_i\, v_i\, \lambda_i(X)$$

Prover sends $[v_i]$, $[(x-\omega^{i-1})]$, $[Q_i(x)]$ s.t:

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

Verifier checks

$$e([C(x)], [v_i])=e([(x-\omega^{i-1})], [Q_i(x)])$$

Prover sends $[C_I(x)]$, $[\Pi_{i\varepsilon I}(x-\omega^{i-1})]$, $[Q_I(x)]$ s.t:

$$C(X)-C_I(X)=\Pi_{i\varepsilon I}\,(X-\omega^{i-1})\,Q_I(X)$$

Verifier checks

$$e([C(x)],\ [C_I(x)])=e([\Pi_{i\varepsilon I}(x-\omega^{i-1})], [Q_I(x)])$$

$Q_i(X)$ and $Q_I(X)$ are linear in N!!!

KZG + TABDFK

Precompute $([Q_1(x)],\ldots,[Q_N(x)])$

KZG + TABDFK

Precompute $([Q_1(x)],\ldots,[Q_N(x)])$

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

KZG + TABDFK

Precompute $([Q_1(x)],\ldots,[Q_N(x)])$

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

KZG + TABDFK

Precompute $([Q_1(x)],\ldots,[Q_N(x)])$

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

$$C(X)-C_I(X)=\Pi_{i\varepsilon I}\,(X-\omega^{i-1})\,Q_I(X)$$

KZG + TABDFK

Precompute $([Q_1(x)],\ldots,[Q_N(x)])$

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

$$\{Q_i(X)\}_{i\varepsilon\, I}$$

$$C(X)-C_I(X)=\Pi_{i\varepsilon\, I}\,(X-\omega^{i-1})\,Q_I(X)$$

KZG + TABDFK

Precompute $([Q_1(x)],\ldots,[Q_N(x)])$

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

$$\{Q_i(X)\}_{i\varepsilon\, I}$$

$$C(X)-C_I(X)=\Pi_{i\varepsilon\, I}\,(X-\omega^{i-1})\,Q_I(X)$$

KZG + TABDFK

Precompute $([Q_1(x)],\ldots,[Q_N(x)])$

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

$$\{Q_i(X)\}_{i\varepsilon I} \qquad Q_I(X)=\Sigma_{i\varepsilon I}\, k_i Q_i(X)$$

$$C(X)-C_I(X)=\Pi_{i\varepsilon I}\,(X-\omega^{i-1})\,Q_I(X)$$

KZG + TABDFK

Precompute $([Q_1(x)],\ldots,[Q_N(x)])$

$$C(X)-v_i=(X-\omega^{i-1})Q_i(X)$$

$$\{Q_i(X)\}_{i\varepsilon I}$$

$$Q_I(X)=\Sigma_{i\varepsilon I}\, k_i Q_i(X)$$

$$C(X)-C_I(X)=\Pi_{i\varepsilon I}\,(X-\omega^{i-1})\,Q_I(X)$$

Prover depends on $|I|=m$

KZG + TABDFK

$C(X)=\Sigma_i\ v_i\ \lambda_i(X)$ is public

$proof_i=([v_i], [(x-\omega^{i-1})], [Q_i(x)])$

$proof_I=([C_I(x)], [\Pi_{i\varepsilon\ I}\ (x-\omega^{i-1})], [Q_I(x)])$

KZG + TABDFK

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

Blind v_i, $C_I(X)$

$proof_i=([v_i], [(x-\omega^{i-1})], [Q_i(x)])$

$proof_I=([C_I(x)], [\Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I(x)])$

CHALLENGES

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

Blind v_i, $C_I(X)$

$proof_i=([v_i+hr], [(x-\omega^{i-1})], [Q_i(x)])$

$proof_I=([C_I(x)+z_I(x)s(x)], [\Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I(x)])$

CHALLENGES

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

Blind v_i, $C_I(X)$

$proof_i=([a], [(x-\omega^{i-1})], [Q_i(x)])$

$proof_I=([a], [\Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I(x)])$

KZG + TABDFK

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

Blind $Q_i(X), Q_I(X)$

$proof_i=([v_i], [(x-\omega^{i-1})], [Q_i(x)])$

$proof_I=([C_I(x)], [\Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I(x)])$

CHALLENGES

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

Blind $Q_i(X), Q_I(X)$

$proof_i=([a], [(x-\omega^{i-1})], [Q_i(x)+sh)])$

$proof_I=([a], [\Pi_{i\varepsilon I} (x-\omega^{i-1})], [r_1^{-1}Q_I(x)+r(x)])$

CHALLENGES

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

Blind $v_i, C_I(X)$

Blind $Q_i(X), Q_I(X)$

$proof_i=([a], [(x-\omega^{i-1})], [Q_i])$

$proof_I=([a], [\Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I])$

KZG + TABDFK

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

$proof_i=([v_i], [(x-\omega^{i-1})], [Q_i])$

Blind , $(X-\omega^{i-1})$, $\Pi_{i\varepsilon I}(X-\omega^{i-1})$

$proof_I=([C_I(x)], [\Pi_{i\varepsilon I}(x-\omega^{i-1})], [Q_I])$

CHALLENGES

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

$proof_i=([a], [a(x-\omega^{i-1})], [Q_i])$

Blind , $(X-\omega^{i-1}), \Pi_{i\varepsilon I} (X-\omega^{i-1})$

$proof_I=([a], [r_1\Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I])$

CHALLENGES

$C(X)=\Sigma_i\ v_i\ \lambda_i(X)$ is public

Blind $v_i, C_I(X)$

Blind $Q_i(X), Q_I(X)$

$proof_i=([a], [z], [Q_i])$

Blind , $(X-\omega^{i-1}), \Pi_{i\varepsilon\ I}\ (X-\omega^{i-1})$

$proof_I=([a], [z_I], [Q_I])$

CHALLENGES

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

$proof_i=([a], [z], [Q_i])$

$proof_I=([a], [z_I], [Q_I])$

- Blind v_i, $C_I(X)$
- Blind $Q_i(X)$, $Q_I(X)$
- Blind , $(X-\omega^{i-1})$, $\Pi_{i\varepsilon I}(X-\omega^{i-1})$
- Well formation

CHALLENGES

$C(X)=\Sigma_i v_i \lambda_i(X)$ is public

$proof_i=([a], [z], [Q_i])$

$proof_I=([a], [z_I], [Q_I])$

- Blind $v_i, C_I(X)$
- Blind $Q_i(X), Q_I(X)$
- Blind , $(X-\omega^{i-1}), \Pi_{i\varepsilon I}(X-\omega^{i-1})$
- Well formation

Well formation

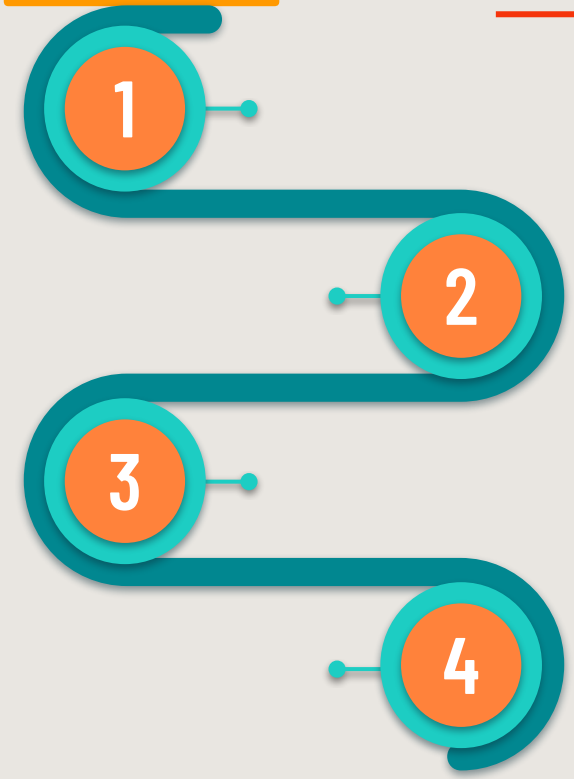
$$[z]=[a(x-\omega^{i-1})]$$

m=1

Well formation

$[z]=[a(x-\omega^{i-1})]$

m=1



Well formation

$[z]=[a(x-\omega^{i-1})]$

m=1

1. Prove $[z]=[ax+b]$ $(b=a\omega^{i-1})$
2.
3.
4.

Well formation

$[z]=[a(x-\omega^{i-1})]$

m=1

1. Prove $[z]=[ax+b]$ $(b=a\omega^{i-1})$

2. Construct f(X) of degree log(N)+6,
   $f(X)=\Sigma_j f_j \mu_j(X)$

3.

4.

Well formation

$[z]=[a(x-\omega^{i-1})]$

m=1

1. Prove $[z]=[ax+b]$ $(b=a\omega^{i-1})$
2. Construct f(X) of degree log(N)+6, $f(X)=\Sigma_j f_j \mu_j(X)$ → New set of roots of unity! V Lagrange polynomials $\{\mu_j(X)\}$
3.
4.

Well formation

$[z]=[a(x-\omega^{i-1})]$

m=1

1. Prove $[z]=[ax+b]$ $(b=a\omega^{i-1})$

2. Construct f(X) of degree log(N)+6,
   $f(X)=\Sigma_j f_j \mu_j(X)$

3. Prove $f_5=b/a$, and for j = 6,...,log(N)+5 $f_j=f_{j-1} f_{j-1}$

4.

Well formation

$[z]=[a(x-\omega^{i-1})]$

m=1

1. Prove $[z]=[ax+b]$ $(b=a\omega^{i-1})$

2. Construct f(X) of degree log(N)+6,
   $f(X)=\Sigma_j f_j \mu_j(X)$

3. Prove $f_5=b/a$, and for j = 6,...,log(N)+5 $f_j=f_{j-1} f_{j-1}$

   Should be ω^{i-1}

4.

Well formation

$[z]=[a(x-\omega^{i-1})]$

m=1

1. Prove $[z]=[ax+b]$ $(b=a\omega^{i-1})$

2. Construct f(X) of degree log(N)+6,
   $f(X)=\Sigma_j f_j \mu_j(X)$

3. Prove $f_5=b/a$, and for j = 6,...,log(N)+5 $f_j=f_{j-1} f_{j-1}$

   Should be ω^{i-1}

   f_{5+j} is the 2^j th power of ω^{i-1}

4.

Well formation

$[z]=[a(x-\omega^{i-1})]$

m=1

1. Prove $[z]=[ax+b]$ $(b=a\omega^{i-1})$

2. Construct f(X) of degree log(N)+6,
   $f(X)=\Sigma_j f_j \mu_j(X)$

3. Prove $f_5=b/a$, and for j = 6,...,log(N)+5 $f_j=f_{j-1} f_{j-1}$

4. Prove $f_{log(N)+5}=1$

Well formation

$[z]=[a(x-\omega^{i-1})]$

m=1

1. Prove $[z]=[ax+b]$ $(b=a\omega^{i-1})$
2. Construct f(X) of degree log(N)+6, $f(X)=\Sigma_j f_j \mu_j(X)$
3. Prove $f_5=b/a$, and for j = 6,...,log(N)+5 $f_j=f_{j-1} f_{j-1}$
4. Prove $f_{\log(N)+5}=1$

$(b/a)^N=1$!!!

m>1

$$proof_I=([C_I(x)],[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})],[Q_I])$$

m>1

$$proof_I=([\Pi_{i\varepsilon I} v_i \tau_i(x)], [r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I])$$

m>1

$$proof_I=([\Pi_{i\varepsilon I} v_i \tau_i(x)], [r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I])$$

$$H_I=\{\omega^{i-1}\}_{i\varepsilon I}$$

m>1

$$proof_I=([\Pi_{i\varepsilon I} v_i \tau_i(x)], [r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I])$$

$$H_I=\{\omega^{i-1}\}_{i\varepsilon I}$$

"I" unknown to the verifier!

$[C(x)=\Sigma_i v_i \lambda_i(x)\,],\ [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([\Pi_{i\varepsilon I} v_i \tau_i(x)], [r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I])$

$[C(x)=\Sigma_i v_i \lambda_i(x)\,], [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([\Pi_{i\varepsilon I} v_i \tau_i(x)], [r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})], [Q_I])$

$a_j=v_i$ for some i, for all j

$[C(x)=\Sigma_i v_i \lambda_i(x)\,], [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

$[C(x)=\Sigma_i v_i \lambda_i(x)\,],\ [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

02

03

04

$[C(x)=\Sigma_i v_i \lambda_i(x)\ ],\ [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

02

03

04

$[C(x)=\Sigma_i v_i \lambda_i(x)\ ], [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

02

03

04

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

1. Set $\mathbf{u}=(\omega^{i-1})_{i\varepsilon I}$ but with repetitions

$[C(x)=\Sigma_i v_i \lambda_i(x)\,], [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

02

03

04

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$

$[C(x)=\Sigma_i v_i \lambda_i(x)\ ], [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

02

03

04

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

The roots used in z_I with repetitions

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$

$[C(x)=\Sigma_i v_i \lambda_i(x)\,], [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

$[z_I]=[r_1 \Pi_{i\varepsilon I}(x-\omega^{i-1})]$

02

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$
2. Compute $\mathbf{u_s=u_{s-1}u_{s-1}}$

03

04

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

02

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$
2. Compute $u_s(X)=u_{s-1}(X)u_{s-1}(X) \bmod z_V(X)$

03

04

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

02

03

04

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$
2. Compute $u_s(X)=u_{s-1}(X)u_{s-1}(X) \bmod z_V(X)$

The coeficients in $u_s(X)$ are the 2^s power of the u_js

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

02

03

04

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$
2. Compute $u_s(X)=u_{s-1}(X)u_{s-1}(X) \bmod z_V(X)$

The coeficients in $u_s(X)$ are the 2^s power of the u_js

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

02

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$
2. Compute $u_s(X)=u_{s-1}(X)u_{s-1}(X) \bmod z_V(X)$
3. Prove $\mathbf{u_{log(N)}}=(1,1,\ldots,1)$

03

04

$[C(x)=\Sigma_i v_i \lambda_i(x)\ ], [\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

02

03

04

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$
2. Compute $u_s(X)=u_{s-1}(X)u_{s-1}(X) \bmod z_V(X)$
3. Prove $u_{log(N)}(X)=\Sigma 1\mu_j(x)$

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

02

03

04

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$
2. Compute $u_s(X)=u_{s-1}(X)u_{s-1}(X) \bmod z_V(X)$
3. Prove $u_{log(N)}(X)=\Sigma 1\mu_j(x)$

All the $2^{log(N)}$ th powers of the u_js are 1!

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

02

03

04

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$

1. Set $u(X)=\Sigma \omega^{i-1} \mu_{j,i}(x)=\Sigma u_j \mu_j(x)$
2. Compute $u_s(X)=u_{s-1}(X)u_{s-1}(X) \bmod z_V(X)$
3. Prove $u_{log(N)}(X)=\Sigma 1\mu_j(x)$

All the Nth powers of the u_js are 1!

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

$[z_I]=[r_1 \Pi_{i\varepsilon I} (x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02

03

04

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02 $e([z_I(u(x))], [1])= e([z_V], [Q_2])$

03

04

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02 $e([z_I(\omega^{something})], [1])= e([0], [Q_2])$

03

04

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01

$[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02

$e([z_I(\omega^{something})], [1])= e([0], [Q_2])$

03

$[z_I]$ is well formed

04

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02 $e([z_I(u(x))], [1])= e([z_V], [Q_2])$

03 $e([C(x)]-[C_I])= e([Q_I], [z_I])$

04

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02 $e([z_I(u(x))], [1])= e([z_V], [Q_2])$

03 $e([C(\omega^{something})]-[C_{Isomething}])= e([Q_I], [0])$

04

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02 $e([z_I(u(x))], [1])= e([z_V], [Q_2])$

03 $e([v_{something}]-[C_{Isomething}])= e([Q_I], [0])$

04

$[C_I]$ contains a *subvector* of **v**

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02 $e([z_I(u(x))], [1])= e([z_V], [Q_2])$

03 $e([C(x)]-[C_I])= e([Q_I], [z_I])$

04 $e([C_I(u(x))]- [\phi(x)], [1])= e([z_V], [Q_3])$

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ $[u(x)]$ with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02 $e([z_I(u(x))], [1])= e([z_V], [Q_2])$

03 $e([C(x)]-[C_I])= e([Q_I], [z_I])$

04 $e([C_I(\omega^{something})]- [a_j], [1])= e([0], [Q_3])$

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02 $e([z_I(u(x))], [1])= e([z_V], [Q_2])$

03 $e([C(x)]-[C_I])= e([Q_I], [z_I])$

04 $e([v_{something})]- [a_j], [1])= [0]$

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

02 $e([z_I(u(x))], [1])= e([z_V], [Q_2])$

03 $e([C(x)]-[C_I])= e([Q_I], [z_I])$

04 $e([v_{something})]- [a_j], [1])= [0]$

Everyting in **a** is also in **v**

$[C(x)=\Sigma_i v_i \lambda_i(x)]$, $[\phi(x)=\Sigma_j a_j \mu_j(x)]$

m>1

$proof_I=([C_I], [z_I], [Q_I])$

01 $[z_I]=[r_1\Pi_{i\varepsilon I}(x-\omega^{i-1})]$ [u(x)] with Nth roots of unity as coefficients in $\{\mu_j(X)\}$

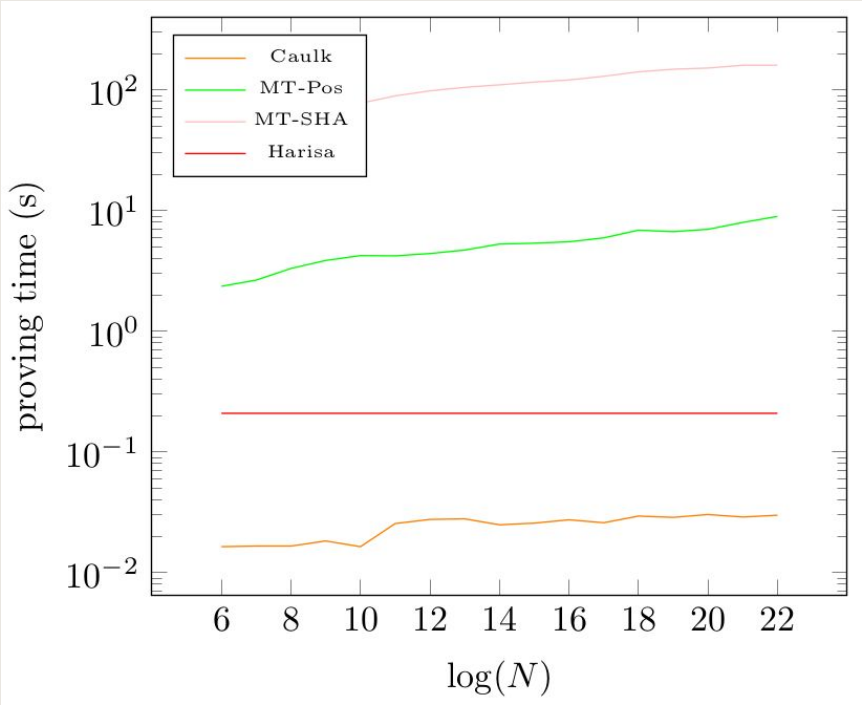
02 $e([z_I(u(x))], [1])= e([z_V], [Q_2])$

03 $e([C(x)]-[C_I])= e([Q_I], [z_I])$

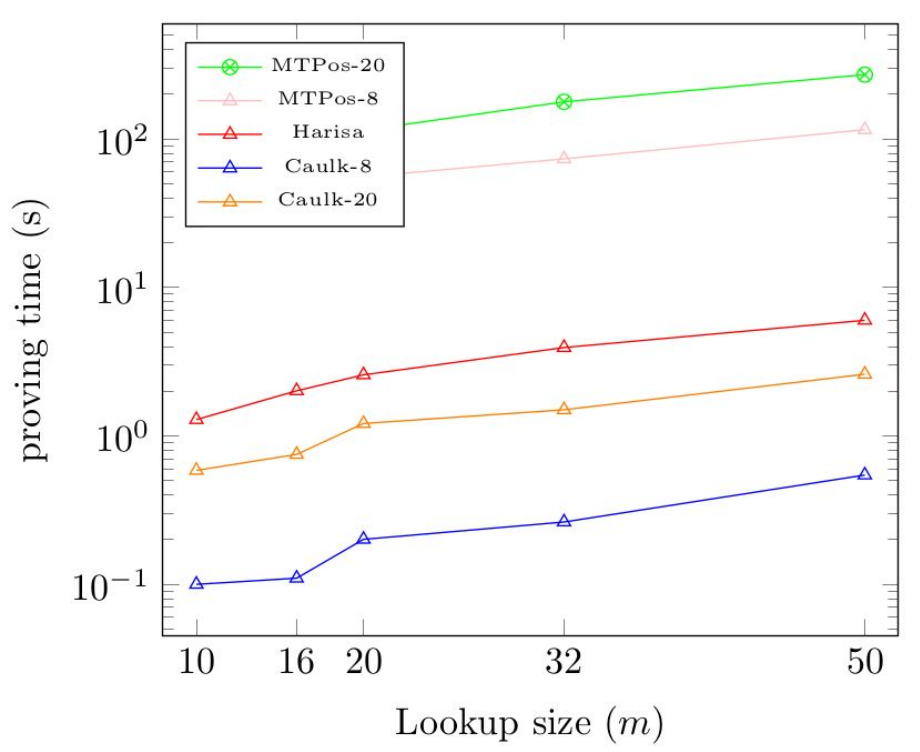
04 $e([v_{something})]- [a_j], [1])= [0]$

Position-hiding linkability!!!

IMPLEMENTATION



IMPLEMENTATION



THANKS!

https://eprint.iacr.org/2022/621