NETHERMIND RESEARCH

Folding over lattices: Performance and implementation

Ilia Vlasov, Marko Čupić, Matthew Klein, Antonio Larriba,
Emanuel Viera, Isaac Villalobos, Albert Garreta

Folding

Folding

- Folding reduces the task of proving 2 instance-witness to proving 1 instance-witness.

NETHERMIND RESEARCH

Folding

- Folding reduces the task of proving 2 instance-witness to proving 1 instance-witness.

- Commitments play a crucial role in folding schemes.

Folding

- Folding reduces the task of proving 2 instance-witness to proving 1 instance-witness.

- Commitments play a crucial role in folding schemes.
- Instances x_1, x_2, x_3 contain a commitment to w_1, w_2, w_3, respectively. I.e.

Folding

- Folding reduces the task of proving 2 instance-witness to proving 1 instance-witness.

- Commitments play a crucial role in folding schemes.
- Instances x_1, x_2, x_3 contain a commitment to w_1, w_2, w_3, respectively. I.e.

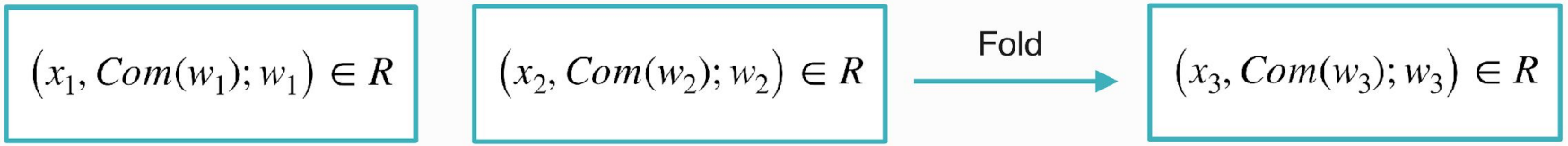
$$(x_i; w_i) = (x_i', Com(w_i); w_i)$$

Folding

- Folding reduces the task of proving 2 instance-witness to proving 1 instance-witness.

- Commitments play a crucial role in folding schemes.
- Instances x_1, x_2, x_3 contain a commitment to w_1, w_2, w_3, respectively. I.e.

$$(x_i; w_i) = (x_i', Com(w_i); w_i)$$



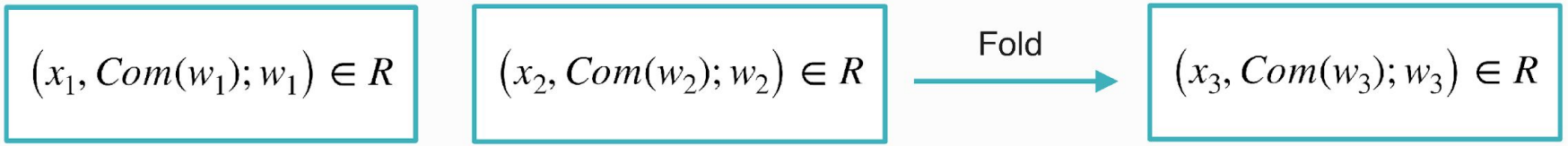
NETHERMIND RESEARCH

Folding

- Folding reduces the task of proving 2 instance-witness to proving 1 instance-witness.

- Commitments play a crucial role in folding schemes.
- Instances x_1, x_2, x_3 contain a commitment to w_1, w_2, w_3, respectively. I.e.

$$(x_i; w_i) = (x_i', Com(w_i); w_i)$$



- Usually* the commitment is homomorphic: $Com(w_1 + w_2) = Com(w_1) + Com(w_2)$

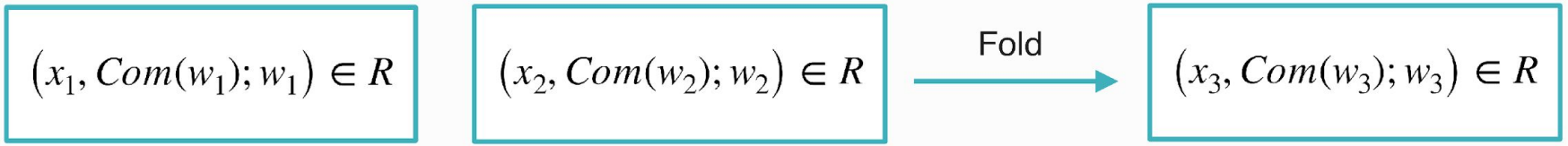
NETHERMIND RESEARCH

Folding

- Folding reduces the task of proving 2 instance-witness to proving 1 instance-witness.

- Commitments play a crucial role in folding schemes.
- Instances x_1, x_2, x_3 contain a commitment to w_1, w_2, w_3, respectively. I.e.

$$(x_i; w_i) = (x_i', Com(w_i); w_i)$$



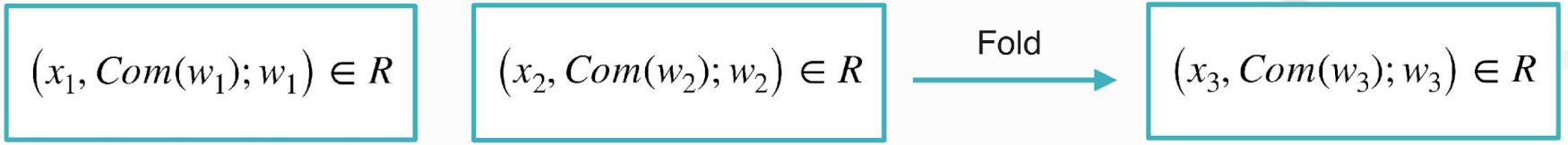
- Usually* the commitment is homomorphic: $Com(w_1 + w_2) = Com(w_1) + Com(w_2)$

*Not in, e.g. Arc (Bünz, Mishra, Nguyen, Wang, 2024)

NETHERMIND RESEARCH

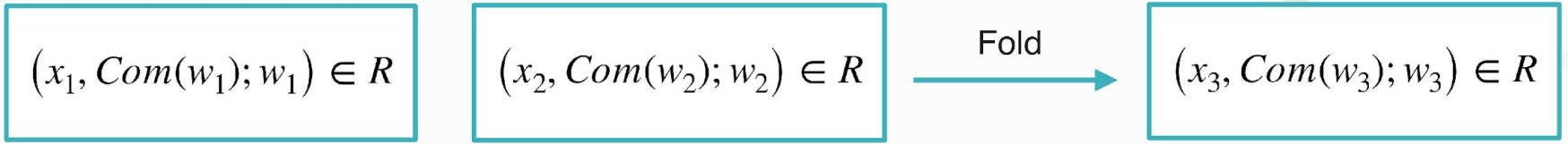
Commitments in folding schemes

Commitments in folding schemes



NETHERMIND RESEARCH

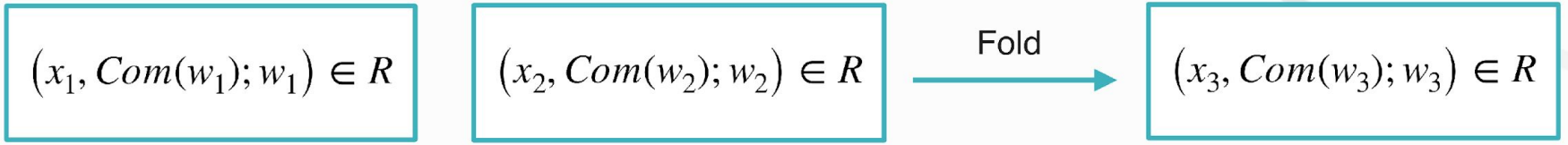
Commitments in folding schemes



- Usually, Com is the Pedersen or KZG scheme (or similar).

NETHERMIND RESEARCH

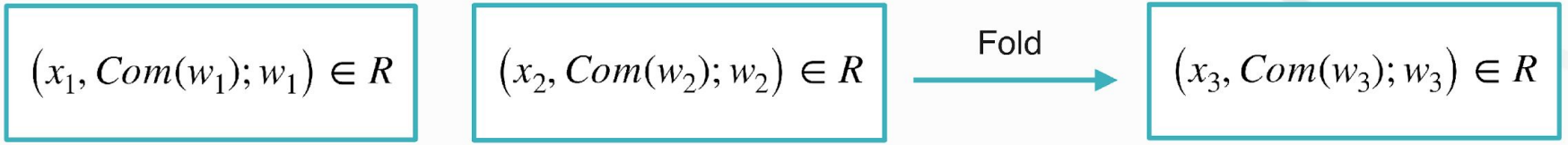
Commitments in folding schemes



- Usually, Com is the Pedersen or KZG scheme (or similar).
- E.g. in Nova, Hypernova, Protostar, Protogalaxy, NeutronNova, KZH, etc.

NETHERMIND RESEARCH

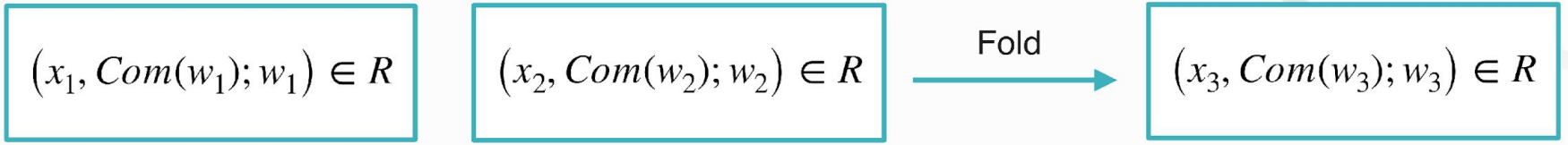
Commitments in folding schemes



- Usually, Com is the Pedersen or KZG scheme (or similar).
- E.g. in Nova, Hypernova, Protostar, Protogalaxy, NeutronNova, KZH, etc.
- Drawbacks:

NETHERMIND RESEARCH

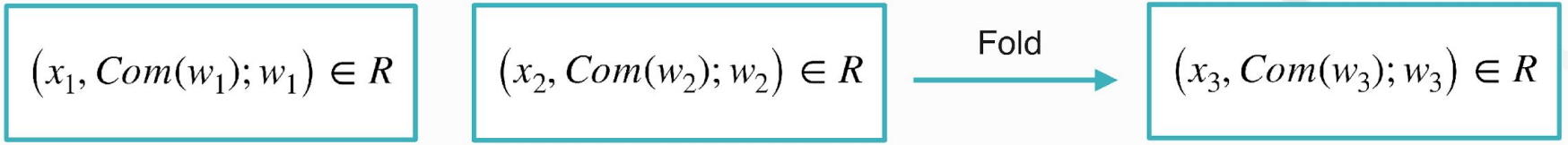
Commitments in folding schemes



- Usually, Com is the Pedersen or KZG scheme (or similar).
- E.g. in Nova, Hypernova, Protostar, Protogalaxy, NeutronNova, KZH, etc.
- Drawbacks:
  - Witness lives in a big field: ≥ 250 bits.

NETHERMIND RESEARCH

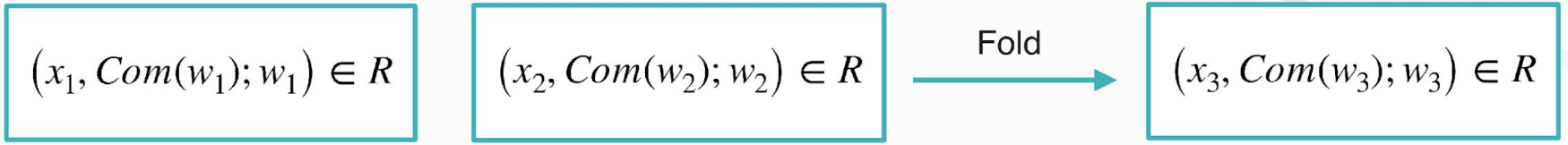
Commitments in folding schemes



- Usually, Com is the Pedersen or KZG scheme (or similar).
- E.g. in Nova, Hypernova, Protostar, Protogalaxy, NeutronNova, KZH, etc.
- Drawbacks:
  - Witness lives in a big field: ≥ 250 bits.
  - Expensive commitment, especially if the vector has large entries.

NETHERMIND RESEARCH

Commitments in folding schemes



- Usually, Com is the Pedersen or KZG scheme (or similar).
- E.g. in Nova, Hypernova, Protostar, Protogalaxy, NeutronNova, KZH, etc.
- Drawbacks:
  - Witness lives in a big field: ≥ 250 bits.
  - Expensive commitment, especially if the vector has large entries.
  - Expensive to recurse over: Proving that folding was performed correctly is complex due to the need of arithmetizing foreign field.

An alternative: lattice-based commitments

An alternative: lattice-based commitments

A cyclotomic ring has the form

An alternative: lattice-based commitments

A cyclotomic ring has the form

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) = \{\text{all polys of deg} < \text{d}\}$$

An alternative: lattice-based commitments

A cyclotomic ring has the form

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) = \{\text{all polys of deg} < \text{d}\}$$

Where $f(X)$ is a cyclotomic polynomial, e.g. $f(X) = X^{2^t} + 1$

An alternative: lattice-based commitments

A cyclotomic ring has the form

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) = \{\text{all polys of deg} < \text{d}\}$$

Where $f(X)$ is a cyclotomic polynomial, e.g. $f(X) = X^{2^t} + 1$

NTT isomorphism

$$\mathscr{R} \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

An alternative: lattice-based commitments

A cyclotomic ring has the form

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) = \{\text{all polys of deg} < \text{d}\}$$

Where $f(X)$ is a cyclotomic polynomial, e.g. $f(X) = X^{2^t} + 1$

τ, t depend on $f(X)$ and q.

NTT isomorphism

$$\mathcal{R} \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

An alternative: lattice-based commitments

A cyclotomic ring has the form

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) = \{\text{all polys of deg} < \text{d}\}$$

Where $f(X)$ is a cyclotomic polynomial, e.g. $f(X) = X^{2^t} + 1$

τ, t depend on $f(X)$ and q.

NTT isomorphism

$$\mathscr{R} \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ring packing

An alternative: lattice-based commitments

A cyclotomic ring has the form

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) = \{\text{all polys of deg} < \text{d}\}$$

Where $f(X)$ is a cyclotomic polynomial, e.g. $f(X) = X^{2^t} + 1$

τ, t depend on $f(X)$ and q.

NTT isomorphism

$$\mathscr{R} \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ring packing

- Every τ field elements $a_1, \ldots, a_\tau \in \mathbb{F}_q$ can be packed into a ring element:

An alternative: lattice-based commitments

A cyclotomic ring has the form

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) = \{\text{all polys of deg} < \text{d}\}$$

Where $f(X)$ is a cyclotomic polynomial, e.g. $f(X) = X^{2^t} + 1$

τ, t depend on $f(X)$ and q.

NTT isomorphism

$$\mathscr{R} \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ring packing

- Every τ field elements $a_1, \ldots, a_\tau \in \mathbb{F}_q$ can be packed into a ring element:

$$NTT^{-1}(a_1, \ldots, a_\tau)$$

An alternative: lattice-based commitments

A cyclotomic ring has the form

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) = \{\text{all polys of deg} < \text{d}\}$$

Where $f(X)$ is a cyclotomic polynomial, e.g. $f(X) = X^{2^t} + 1$

τ, t depend on $f(X)$ and q.

NTT isomorphism

$$\mathscr{R} \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ring packing

- Every τ field elements $a_1, \ldots, a_\tau \in \mathbb{F}_q$ can be packed into a ring element:

$$NTT^{-1}(a_1, \ldots, a_\tau)$$

- Hence, each ring element may encode τ field witness elements, e.g. τ trace cells

An alternative: lattice-based commitments

A cyclotomic ring has the form

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) = \{\text{all polys of deg} < \text{d}\}$$

Where $f(X)$ is a cyclotomic polynomial, e.g. $f(X) = X^{2^t} + 1$

τ, t depend on $f(X)$ and q.

NTT isomorphism

$$\mathscr{R} \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ring packing

- Every τ field elements $a_1, \ldots, a_\tau \in \mathbb{F}_q$ can be packed into a ring element:

$$NTT^{-1}(a_1, \ldots, a_\tau)$$

- Hence, each ring element may encode τ field witness elements, e.g. τ trace cells
- Relevant for assessing performance of lattice-based folding

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathscr{R}^{\kappa \times n}$.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\cdots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathscr{R}^{\kappa \times n}$.
- Commitment: Input $v \in \mathscr{R}^n$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\cdots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathscr{R}^{\kappa \times n}$.
- Commitment: Input $v \in \mathscr{R}^n$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Only binding if v has norm $\|\vec{v}\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathscr{R}^{\kappa \times n}$.
- Commitment: Input $v \in \mathscr{R}^n$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Only binding if v has norm $\|\vec{v}\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

Norm of v is largest coeff. of an entry in v, seen as a polynomial in $\mathscr{R}$

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\cdots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- Commitment: Input $v \in \mathscr{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

An alternative: lattice-based commitments

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathcal{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathcal{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathcal{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\cdots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathscr{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

Norm of v is largest coeff. of an entry in v, seen as a polynomial in $\mathscr{R}$

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\cdots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathscr{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

Norm of v is largest coeff. of an entry in v, seen as a polynomial in $\mathscr{R}$

To commit to vectors v of large norm, decompose

An alternative: lattice-based commitments

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathcal{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathcal{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathcal{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

Norm of v is largest coeff. of an entry in v, seen as a polynomial in $\mathcal{R}$

To commit to vectors v of large norm, decompose

$$v = v_1 + Bv_2 + \ldots + B^{t-1}v_t, \text{ with } \|v_i\| \leq B$$

An alternative: lattice-based commitments

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathcal{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathcal{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathcal{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

Norm of v is largest coeff. of an entry in v, seen as a polynomial in $\mathcal{R}$

To commit to vectors v of large norm, decompose

$$v = v_1 + Bv_2 + \ldots + B^{t-1}v_t, \text{ with } \|v_i\| \leq B$$

and commit the v_i's.

An alternative: lattice-based commitments

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathcal{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathcal{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathcal{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

Norm of v is largest coeff. of an entry in v, seen as a polynomial in $\mathcal{R}$

To commit to vectors v of large norm, decompose

$$v = v_1 + Bv_2 + \ldots + B^{t-1}v_t, \text{ with } \|v_i\| \leq B$$

and commit the v_i's.

Tradeoff: number κ of rows in A and how low-norm vectors need to be.

An alternative: lattice-based commitments

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathcal{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathcal{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathcal{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

Norm of v is largest coeff. of an entry in v, seen as a polynomial in $\mathcal{R}$

To commit to vectors v of large norm, decompose

$$v = v_1 + Bv_2 + \ldots + B^{t-1}v_t, \text{ with } \|v_i\| \leq B$$

and commit the v_i's.

Tradeoff: number κ of rows in A and how low-norm vectors need to be.

In some cases, v has low norm naturally.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathscr{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

Norm of v is largest coeff. of an entry in v, seen as a polynomial in $\mathscr{R}$

To commit to vectors v of large norm, decompose

$$v = v_1 + Bv_2 + \ldots + B^{t-1}v_t, \text{ with } \|v_i\| \leq B$$

and commit the v_i's.

Tradeoff: number κ of rows in A and how low-norm vectors need to be.

In some cases, v has low norm naturally.

E.g. in Latticefold+ (Boneh, Chen, 2025) there's commitments to vectors full of elements of the form X^u.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathscr{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\cdots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathscr{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

So, it is homomorphic in some sense, but not homomorphic in some other.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- **Parameters**: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- **Commitment**: Input $v \in \mathscr{R}^m$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Only binding if v has norm $\|v\| < B$ for certain $B = O(2^{\sqrt{\kappa}})$.

So, it is homomorphic in some sense, but not homomorphic in some other.

$A \cdot (v+u)^\mathsf{T} = A \cdot v^\mathsf{T} + A \cdot u^\mathsf{T}$, but maybe $\|v+u\| > B$.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\cdots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- Commitment: Input $v \in \mathscr{R}^n$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\cdots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- Commitment: Input $v \in \mathscr{R}^n$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Boons of Ajtai commitments:

An alternative: lattice-based commitments

$$\mathscr{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathscr{R}^{\kappa \times m}$.
- Commitment: Input $v \in \mathscr{R}^n$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathscr{R}^\kappa$.

Boons of Ajtai commitments:

$\mathbb{F}_q$ can be a small field: $q \approx 32,64$ bits, including STARK primes (Goldilocks, Babybear).

An alternative: lattice-based commitments

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\cdots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathcal{R}^{\kappa \times m}$.
- Commitment: Input $v \in \mathcal{R}^n$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathcal{R}^\kappa$.

Boons of Ajtai commitments:

$\mathbb{F}_q$ can be a small field: $q \approx 32,64$ bits, including STARK primes (Goldilocks, Babybear).

Each ring element can pack τ field elements.

An alternative: lattice-based commitments

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathcal{R}^{\kappa \times m}$.
- Commitment: Input $v \in \mathcal{R}^n$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathcal{R}^\kappa$.

Boons of Ajtai commitments:

$\mathbb{F}_q$ can be a small field: $q \approx 32,64$ bits, including STARK primes (Goldilocks, Babybear).

Each ring element can pack τ field elements.

Commit computation should be easily arithmetizable over $\mathbb{F}_q$.

An alternative: lattice-based commitments

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathcal{R}^{\kappa \times m}$.
- Commitment: Input $v \in \mathcal{R}^n$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathcal{R}^\kappa$.

Boons of Ajtai commitments:

$\mathbb{F}_q$ can be a small field: $q \approx 32,64$ bits, including STARK primes (Goldilocks, Babybear).

Each ring element can pack τ field elements.

Commit computation should be easily arithmetizable over $\mathbb{F}_q$.

Plausibly PQ secure.

An alternative: lattice-based commitments

$$\mathcal{R} = \mathbb{F}_q[X]/(f(X)) \cong \mathbb{F}_{q^t} \times \overset{\tau}{\ldots} \times \mathbb{F}_{q^t}$$

Ajtai commitments

- Parameters: A random matrix $A \in \mathcal{R}^{\kappa \times m}$.
- Commitment: Input $v \in \mathcal{R}^n$ with $\|v\| \leq B$. Output $A \cdot v^T \in \mathcal{R}^\kappa$.

Boons of Ajtai commitments:

$\mathbb{F}_q$ can be a small field: $q \approx 32,64$ bits, including STARK primes (Goldilocks, Babybear).

Each ring element can pack τ field elements.

Commit computation should be easily arithmetizable over $\mathbb{F}_q$.

Plausibly PQ secure.

Commitments can be cheap (see next).

Efficiency of Ajtai

Efficiency of Ajtai

Configuration

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

- Vectors of size 2^n stores $8 \cdot 2^n = 2^{n+3}$ elements of $\mathbb{F}_{q^3}$.

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

- Vectors of size 2^n stores $8 \cdot 2^n = 2^{n+3}$ elements of $\mathbb{F}_{q^3}$.
- $B = 2^8$, so committing to a vector in R potentially requires committing to 8 vectors.

Intel 12700F 4.9GHz, 32 GB of RAM

NETHERMIND RESEARCH

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

- v is given in NTT form.

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

- v is given in NTT form.
- And the entries of A

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathcal{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathcal{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathcal{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

- v is given in NTT form.

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathcal{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathcal{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathcal{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

- v is given in NTT form.
- And the entries of A

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

- v is given in NTT form.
- And the entries of A
- Note MT is usually computed on an encoding of v. May make sense using $\rho^{-1} |v|$ size as reference for them.

NETHERMIND RESEARCH

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Two scenarios.

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Two scenarios.

If v has small norm:

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Two scenarios.

If v has small norm:

- About 2x faster than MT-Keccak

NETHERMIND RESEARCH

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Two scenarios.

If v has small norm:

- About 2x faster than MT-Keccak (Depending if we use $\rho^{-1}|v|$ as reference)

NETHERMIND RESEARCH

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Two scenarios.

If v has small norm:

- About 2x faster than MT-Keccak (Depending if we use $\rho^{-1}|v|$ as reference)
- >500x faster than MT-Poseidon

NETHERMIND RESEARCH

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Two scenarios.

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Two scenarios.

If v has large norm:

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Two scenarios.

If v has large norm:

- >1.5-3x slower than MT-Keccac

NETHERMIND RESEARCH

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time	NTT	iNTT
Ajtai	2^16	76ms (0.6s)	10ms	12ms
MT (Keccac)	2^16	21ms	-	-
MT (Keccac)	2^17	44ms	-	-
MT (Keccac)	2^19	185ms	-	-
MT (Keccac)	2^20	387ms	-	-
MT (Poseidon)	2^16	5s	-	-
MT (Poseidon)	2^19	43s	-	-

Intel 12700F 4.9GHz, 32 GB of RAM

Two scenarios.

If v has large norm:

- >1.5-3x slower than MT-Keccac
- >70x faster than MT-Poseidon

NETHERMIND RESEARCH

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)
Pedersen (small entries)	2^16	41ms

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

NETHERMIND RESEARCH

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)
Pedersen (small entries)	2^16	41ms
Pedersen (small entries)	2^19	289ms

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)
Pedersen (small entries)	2^16	41ms
Pedersen (small entries)	2^19	289ms
Pedersen (large entries)	2^16	533ms

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)
Pedersen (small entries)	2^16	41ms
Pedersen (small entries)	2^19	289ms
Pedersen (large entries)	2^16	533ms
Pedersen (large entries)	2^19	2.6s

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathcal{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathcal{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathcal{R}^{\kappa}$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)
Pedersen (small entries)	2^16	41ms
Pedersen (small entries)	2^19	289ms
Pedersen (large entries)	2^16	533ms
Pedersen (large entries)	2^19	2.6s

If v small norm:

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)
Pedersen (small entries)	2^16	41ms
Pedersen (small entries)	2^19	289ms
Pedersen (large entries)	2^16	533ms
Pedersen (large entries)	2^19	2.6s

If v small norm:

- 7-30x faster than Pedersen

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)
Pedersen (small entries)	2^16	41ms
Pedersen (small entries)	2^19	289ms
Pedersen (large entries)	2^16	533ms
Pedersen (large entries)	2^19	2.6s

If v small norm:

- 7-30x faster than Pedersen

If v large norm:

Intel 12700F 4.9GHz, 32 GB of RAM

Efficiency of Ajtai

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Ajtai commitment:

- Parameters: $A \in \mathscr{R}^{\kappa \times m}$
- Commitment: $A \cdot v^T \in \mathscr{R}^{\kappa}$.

	|v|	Commit time
Ajtai	2^16	76ms (0.6s)
Pedersen (small entries)	2^16	41ms
Pedersen (small entries)	2^19	289ms
Pedersen (large entries)	2^16	533ms
Pedersen (large entries)	2^19	2.6s

If v small norm:

- 7-30x faster than Pedersen

If v large norm:

- 0.5-4.3x faster than Pedersen

Intel 12700F 4.9GHz, 32 GB of RAM

Latticefold

Latticefold

Latticefold (Boneh, Chen, 2024)

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Decomposition

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathcal{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Decomposition

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathcal{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Decomposition

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Problem: Maybe $\|w_1 + \alpha w_2\| > B$ even if $\|w_1\|, \|w_2\| \leq B$

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathcal{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Decomposition

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Problem: Maybe $\|w_1 + \alpha w_2\| > B$ even if $\|w_1\|, \|w_2\| \leq B$

LF solution: Split w_1, w_2 into vectors of small norm, commit to them, and take linear combination of these.

Latticefold

Experiments

$|w_1|, |w_2| = 2^{16}$

LF cost: 3s

LF+ expected cost: 0.4s

Decomposition

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Problem: Maybe $\|w_1 + \alpha w_2\| > B$ even if $\|w_1\|, \|w_2\| \leq B$

LF solution: Split w_1, w_2 into vectors of small norm, commit to them, and take linear combination of these.

Latticefold

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathcal{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Experiments

$|w_1|, |w_2| = 2^{16}$

LF cost: 3s

LF+ expected cost: 0.4s

Decomposition

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Problem: Maybe $\|w_1 + \alpha w_2\| > B$ even if $\|w_1\|, \|w_2\| \leq B$

LF solution: Split w_1, w_2 into vectors of small norm, commit to them, and take linear combination of these.

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Norm bound enforcement

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathcal{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Norm bound enforcement

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathcal{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Norm bound enforcement

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Problem: We need extractor to output w_1, w_2 with $\|w_1\|, \|w_2\| \leq B$

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathcal{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Norm bound enforcement

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Problem: We need extractor to output w_1, w_2 with $\|w_1\|, \|w_2\| \leq B$

LF solution: Add a range check during the folding step.

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathcal{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Norm bound enforcement

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Problem: We need extractor to output w_1, w_2 with $\|w_1\|, \|w_2\| \leq B$

LF solution: Add a range check during the folding step.

Range check performed by running a sumcheck per chunk committed in the decomposition step

Latticefold

Experiments

$|w_1|, |w_2| = 2^{16}$

LF cost: 3s

LF+ expected cost: 0.6-1s

Norm bound enforcement

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Problem: We need extractor to output w_1, w_2 with $\|w_1\|, \|w_2\| \leq B$

LF solution: Add a range check during the folding step.

Range check performed by running a sumcheck per chunk committed in the decomposition step

Latticefold

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathcal{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Experiments

$|w_1|, |w_2| = 2^{16}$

LF cost: 3s

LF+ expected cost: 0.6-1s

Norm bound enforcement

To fold two witnesses w_1, w_2, one usually takes a linear combination $w_1 + \alpha w_2$

Problem: We need extractor to output w_1, w_2 with $\|w_1\|, \|w_2\| \leq B$

LF solution: Add a range check during the folding step.

Range check performed by running a sumcheck per chunk committed in the decomposition step

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Linearization

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Linearization

Transforms CCS into a claim about evaluations of certain multilinear polynomials

Latticefold

Latticefold (Boneh, Chen, 2024)

- Folding scheme for CCS relations over $\mathscr{R}$
- Uses Ajtai commitments
- Consists of three parts
  - Linearization (analogous to Hypernova)
  - Decomposition
  - Norm bound enforcement (done during the folding phase, in LF's terminology)

Linearization

Transforms CCS into a claim about evaluations of certain multilinear polynomials

Analogous to Hypernova's linearization

Latticefold

Experiments

$|w_1|, |w_2| = 2^{16}$

LF cost: 170ms

LF+ expected cost: 170ms

Linearization

Transforms CCS into a claim about evaluations of certain multilinear polynomials

Analogous to Hypernova's linearization

Latticefold

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathcal{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Experiments

$|w_1|, |w_2| = 2^{16}$

LF cost: 170ms

LF+ expected cost: 170ms

Linearization

Transforms CCS into a claim about evaluations of certain multilinear polynomials

Analogous to Hypernova's linearization

Overall costs

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Latticefold

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness
2^13

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|
2^13	2^16

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize
2^13	2^16	170ms

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp
2^13	2^16	170ms	3s

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound
2^13	2^16	170ms	3s	3s

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness
2^13

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|
2^13	2^16

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|	Linearize
2^13	2^16	170ms

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|	Linearize	LF+ decomp
2^13	2^16	170ms	~400ms

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|	Linearize	LF+ decomp	LF norm bound
2^13	2^16	170ms	~400ms	~600ms

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|	Linearize	LF+ decomp	LF norm bound	Total
2^13	2^16	170ms	~400ms	~600ms	~1.17s

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|	Linearize	LF+ decomp	LF norm bound	Total
2^13	2^16	170ms	~400ms	~600ms	~1.17s

Hypernova (from Sonobe implementation)

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|	Linearize	LF+ decomp	LF norm bound	Total
2^13	2^16	170ms	~400ms	~600ms	~1.17s

Hypernova (from Sonobe implementation)

CCS witness	Total
2^16	1.2s

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Latticefold

CCS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|	Linearize	LF+ decomp	LF norm bound	Total
2^13	2^16	170ms	~400ms	~600ms	~1.17s

Hypernova (from Sonobe implementation)

CCS witness	Total
2^16	1.2s

Neo (Nguyen, Setty, 2025)

WIP! (Very promising as well)

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

Thanks

. bits), $q \approx 2^{64}$.

$-X^{12}+1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

and $B = 2^8$.

Latticefold

CCS witr

	LF norm bound	Total
3s	3s	6.17s

..ed, speculative)

	..nearize	LF+ decomp	LF norm bound	Total
..16	170ms	~400ms	~600ms	~1.17s

..nova (from Sonobe implementation)

CCS witness	Total
2^16	1.2s

Benchmarks

Repo

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

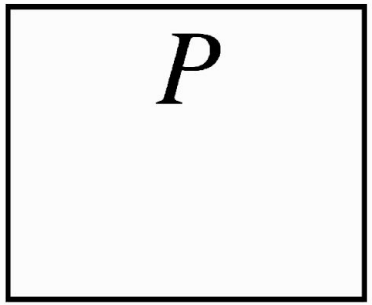
A toy folding scheme

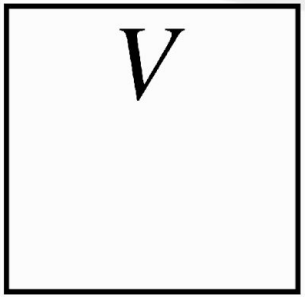
A toy folding scheme

$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.

A toy folding scheme

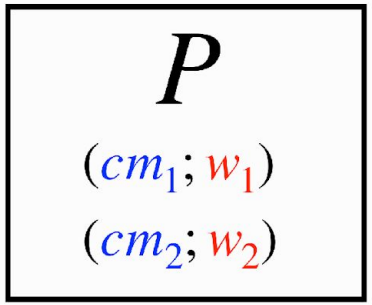
$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.

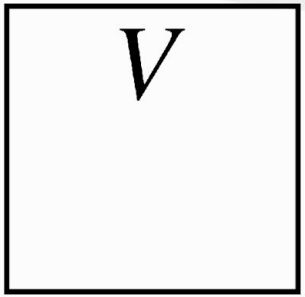




A toy folding scheme

$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.

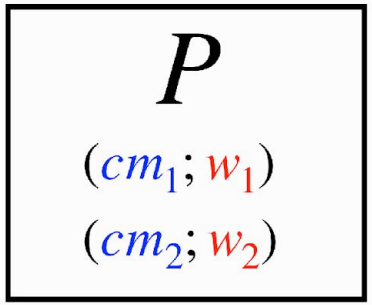


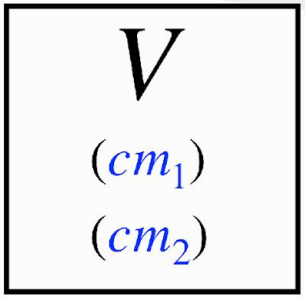


NETHERMIND RESEARCH

A toy folding scheme

$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.

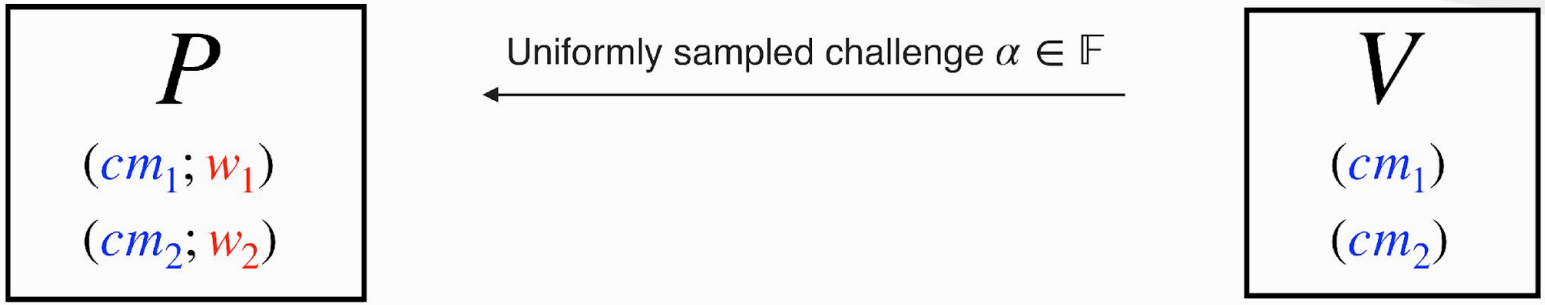




NETHERMIND RESEARCH

A toy folding scheme

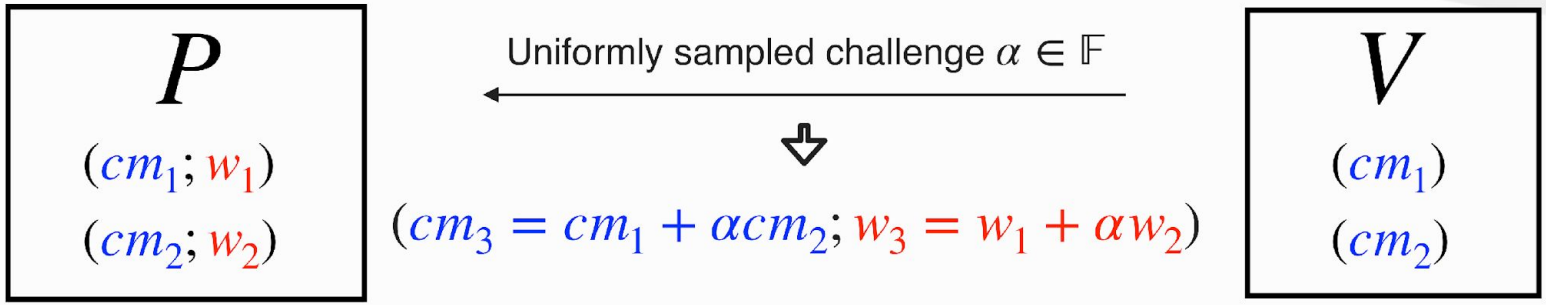
$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.



NETHERMIND RESEARCH

A toy folding scheme

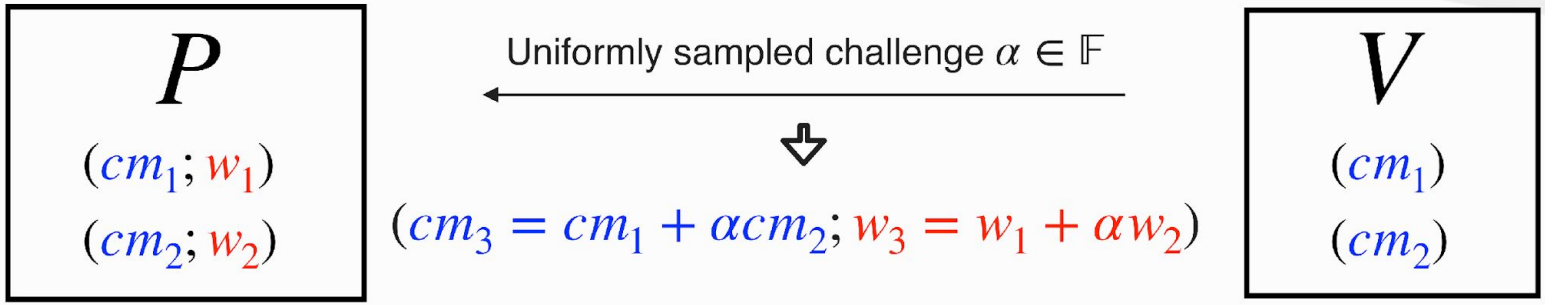
$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.



NETHERMIND RESEARCH

A toy folding scheme

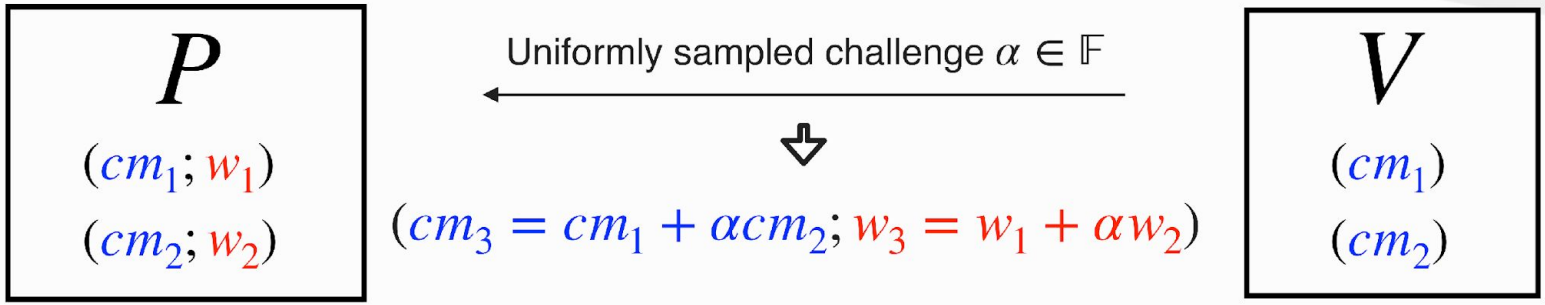
$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.



Does not work when Com is the Ajtai commitment.

A toy folding scheme

$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.

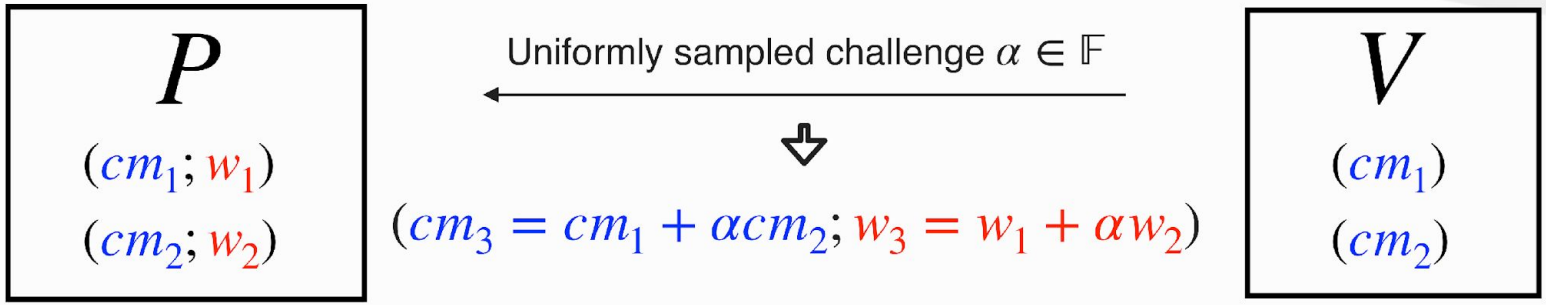


Does not work when Com is the Ajtai commitment.

Problem 1

A toy folding scheme

$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.



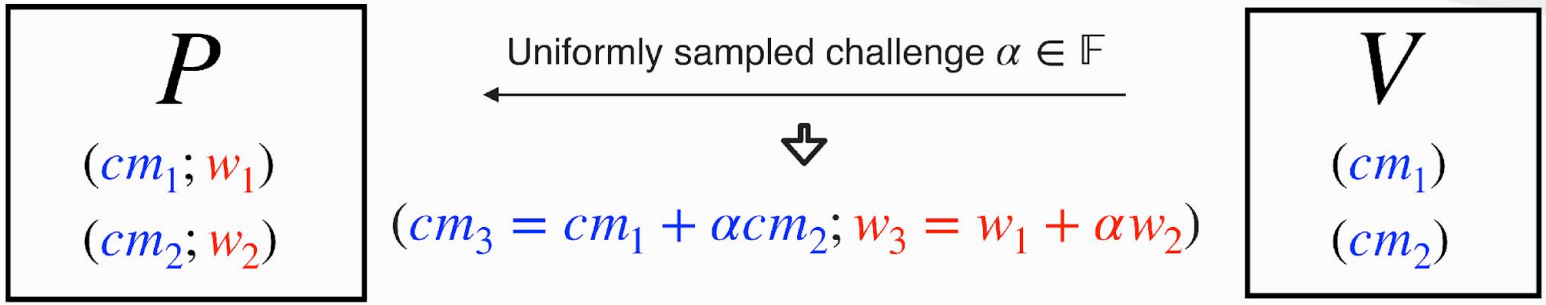
Does not work when Com is the Ajtai commitment.

Problem 1

Need to ask that $\|w\| \leq B$.

A toy folding scheme

$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.



Does not work when Com is the Ajtai commitment.

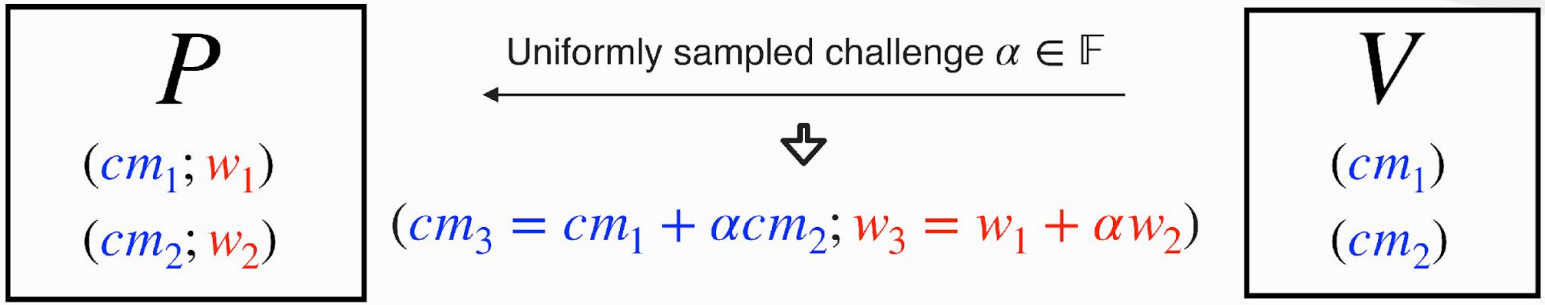
Problem 1

Need to ask that $\|w\| \leq B$.

$R_B = \{(cm; w) \mid Com(w) = cm, \ \|w\| \leq B\}$

A toy folding scheme

$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.



Does not work when Com is the Ajtai commitment.

Problem 1

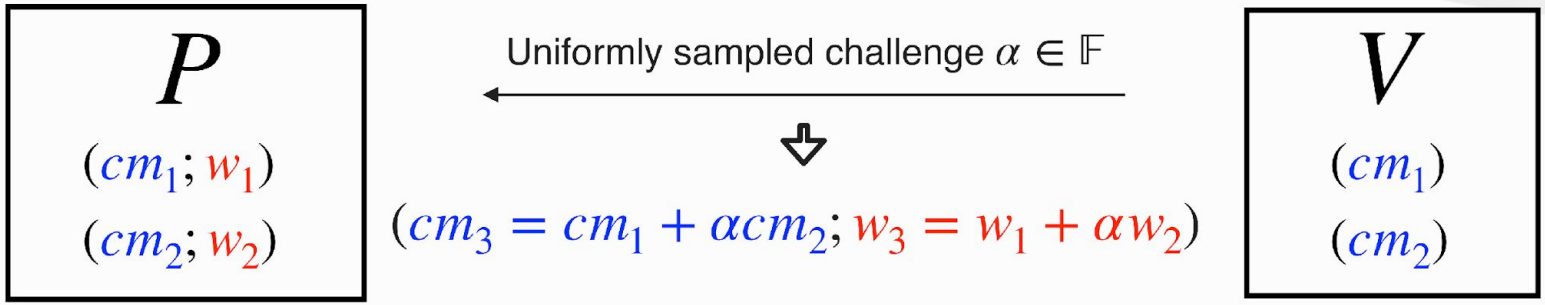
Need to ask that $\|w\| \leq B$.

$R_B = \{(cm; w) \mid Com(w) = cm, \ \|w\| \leq B\}$

Problem 2

A toy folding scheme

$R = \{(cm; w) \mid Com(w) = cm\}$, Com homomorphic commitment scheme.



Does not work when Com is the Ajtai commitment.

Problem 1

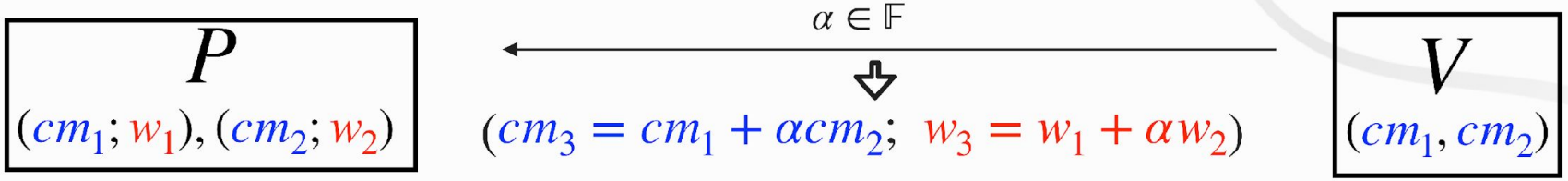
Need to ask that $\|w\| \leq B$.

$R_B = \{(cm; w) \mid Com(w) = cm, \ \|w\| \leq B\}$

Problem 2

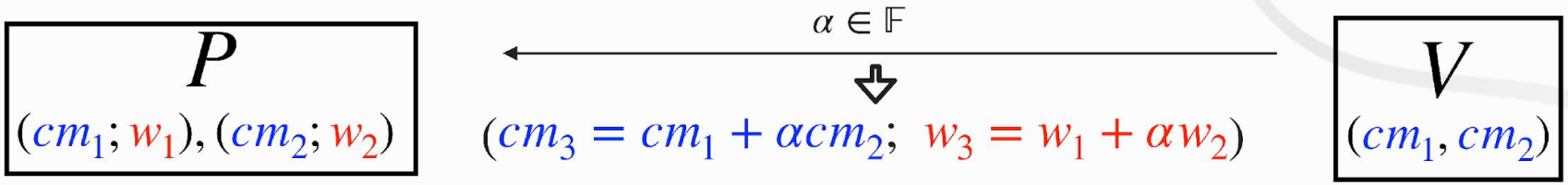
Maybe $\|w_1 + \alpha w_2\| > B$.

Solving norm increases



NETHERMIND RESEARCH

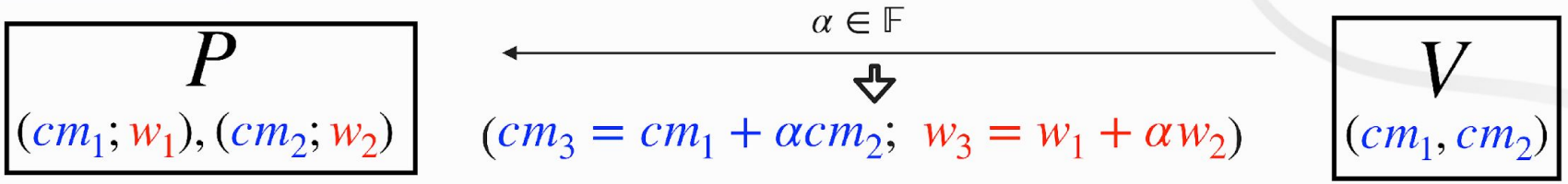
Solving norm increases



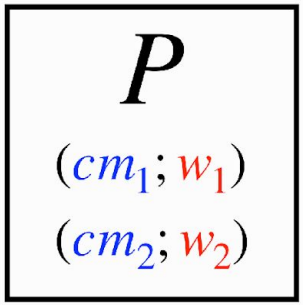
Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$

NETHERMIND RESEARCH

Solving norm increases

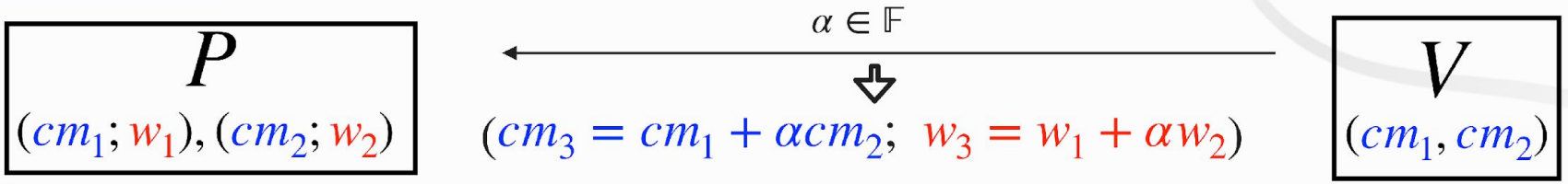


Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$

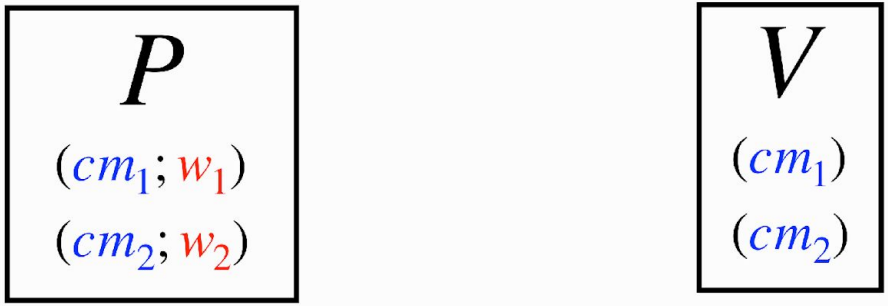


NETHERMIND RESEARCH

Solving norm increases

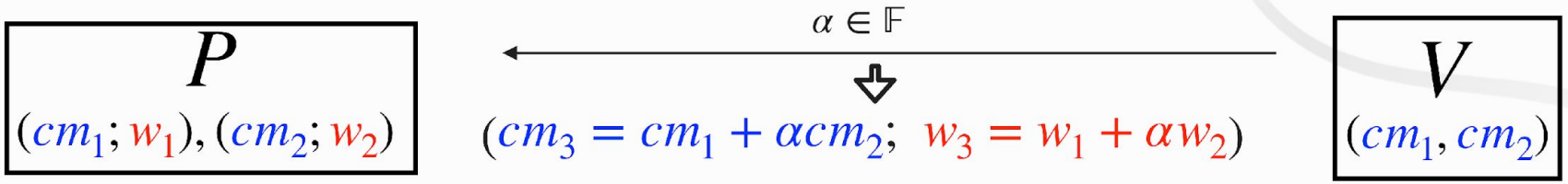


Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



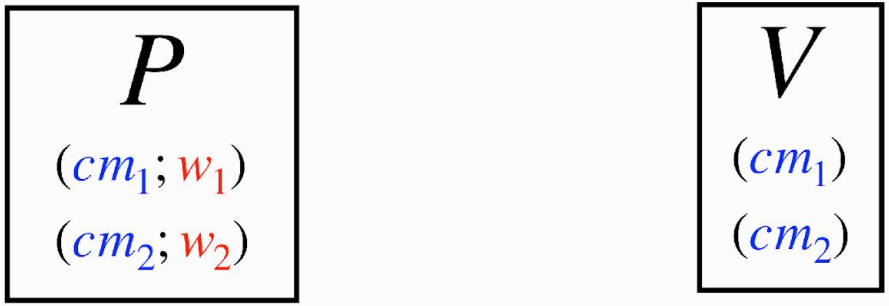
NETHERMIND RESEARCH

Solving norm increases



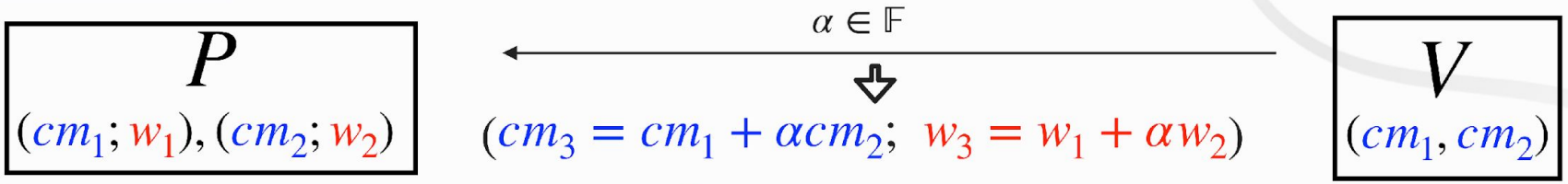
Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$

Solution (Latticefold)



NETHERMIND RESEARCH

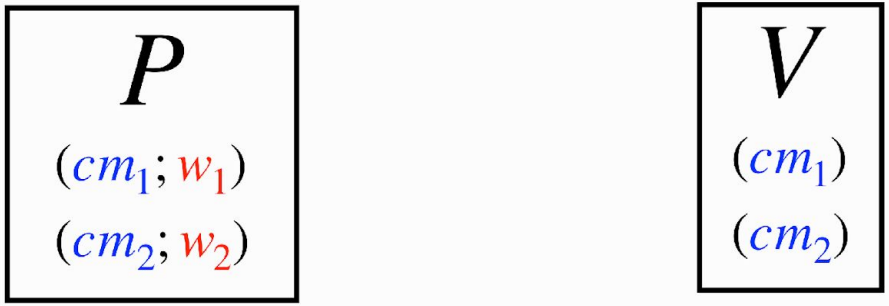
Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$

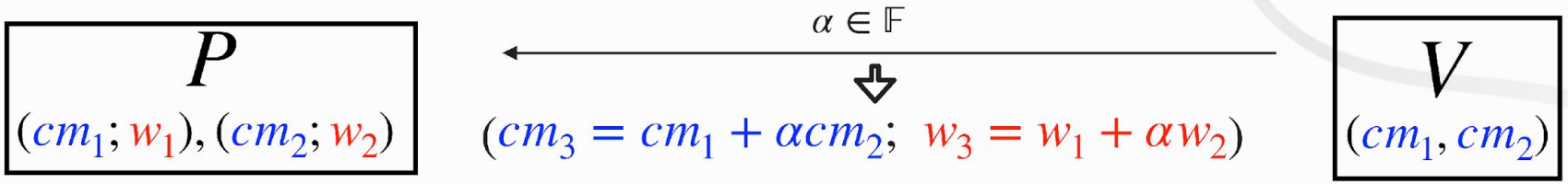
Solution (Latticefold)

P writes $b^2 = B$ and

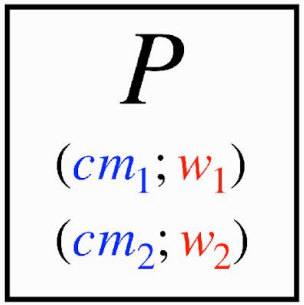


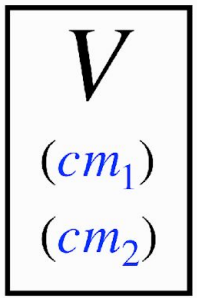
NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



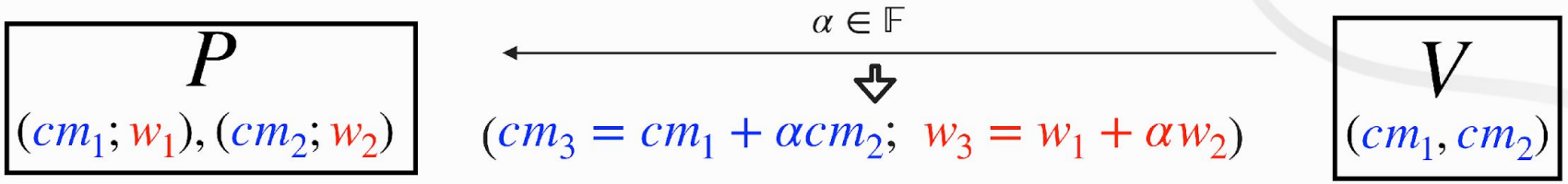


Solution (Latticefold)

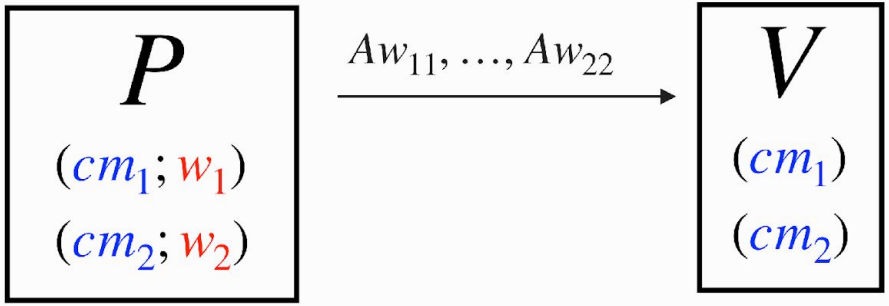
P writes $b^2 = B$ and

$$w_1 = w_{11} + w_{12} b$$
$$w_2 = w_{21} + w_{22} b$$

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$

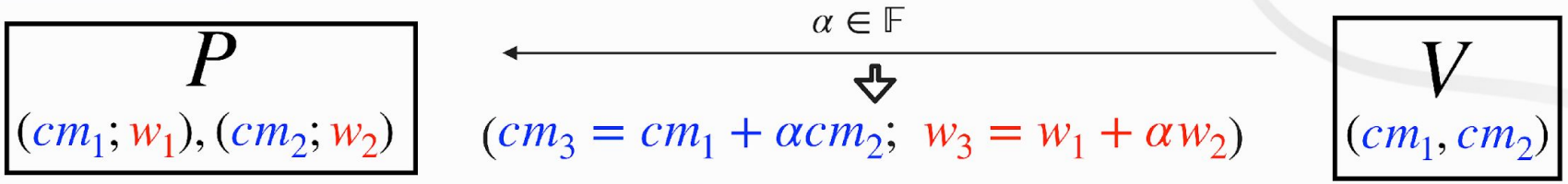


Solution (Latticefold)

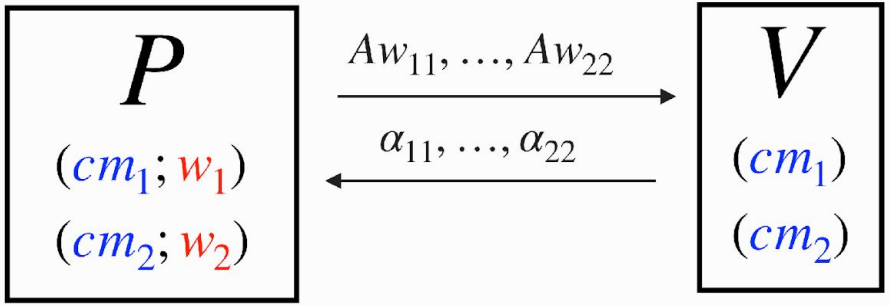
P writes $b^2 = B$ and

$$w_1 = w_{11} + w_{12} b$$
$$w_2 = w_{21} + w_{22} b$$

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



Solution (Latticefold)

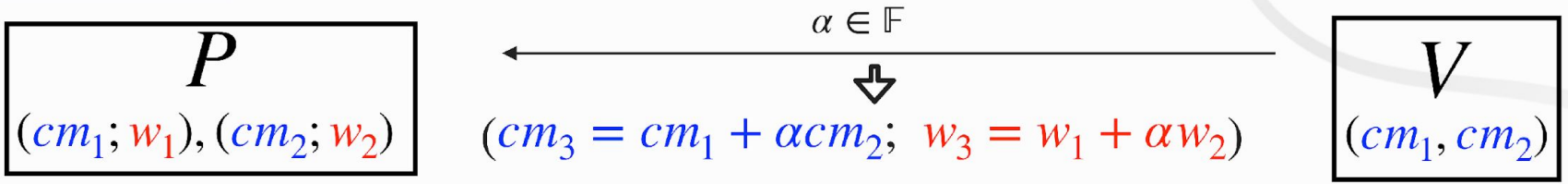
P writes $b^2 = B$ and

$$w_1 = w_{11} + w_{12}b$$

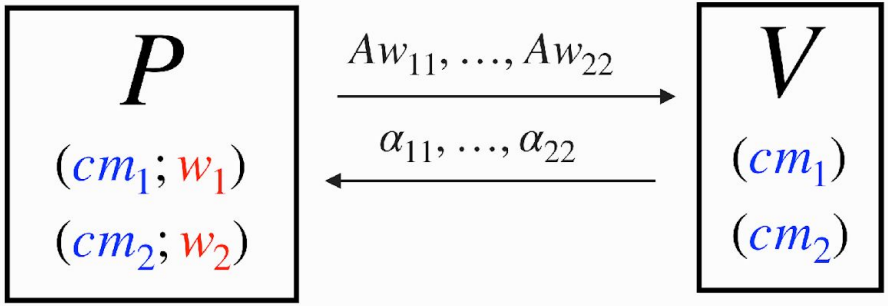
$$w_2 = w_{21} + w_{22}b$$

V sends $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ sampled in certain subset of $\mathcal{R}$ that guarantees

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



Solution (Latticefold)

P writes $b^2 = B$ and

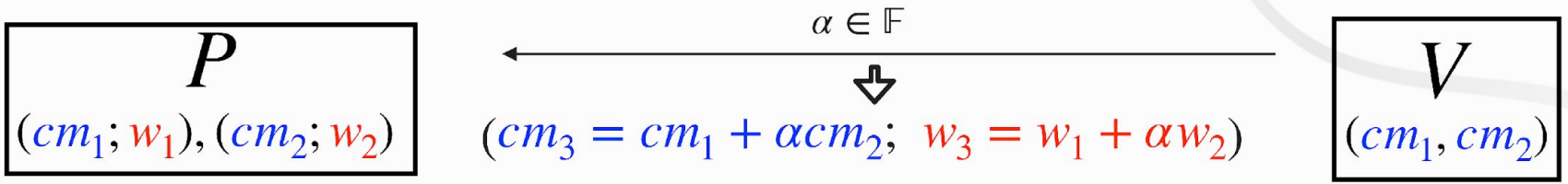
$$w_1 = w_{11} + w_{12}b$$

$$w_2 = w_{21} + w_{22}b$$

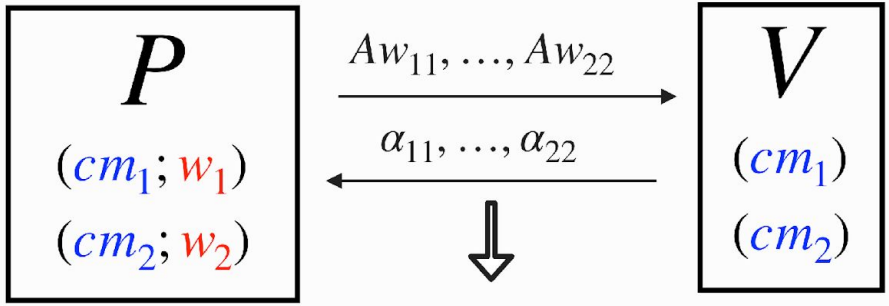
V sends $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ sampled in certain subset of $\mathcal{R}$ that guarantees

$$\|\alpha_{11}w_{11} + \ldots + \alpha_{22}w_{22}\| \leq B$$

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\left(\begin{array}{c} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{array}\right)$$

Solution (Latticefold)

P writes $b^2 = B$ and

$$w_1 = w_{11} + w_{12} b$$

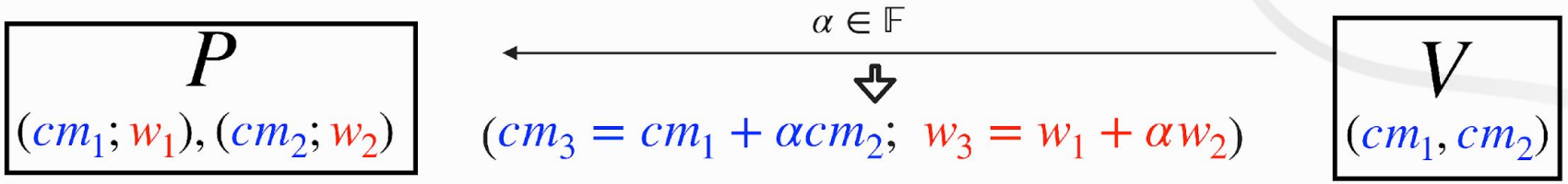
$$w_2 = w_{21} + w_{22} b$$

V sends $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ sampled in certain subset of $\mathcal{R}$ that guarantees

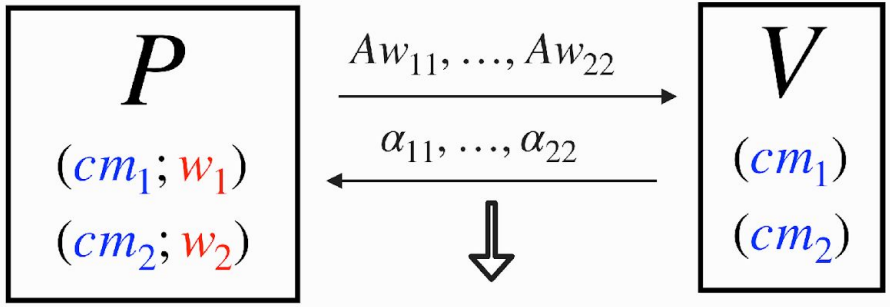
$$\|\alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22}\| \leq B$$

NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\left(\begin{array}{c} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{array}\right)$$

Solution (Latticefold)

P writes $b^2 = B$ and

$$w_1 = w_{11} + w_{12} b$$

$$w_2 = w_{21} + w_{22} b$$

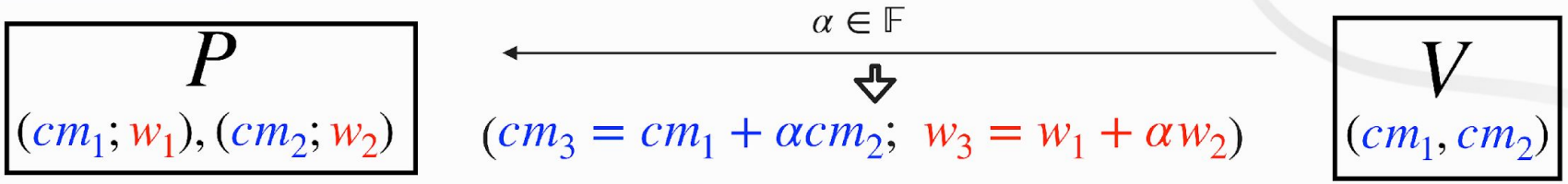
V sends $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ sampled in certain subset of $\mathcal{R}$ that guarantees

$$\|\alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22}\| \leq B$$

Call the w_{ij} chunks

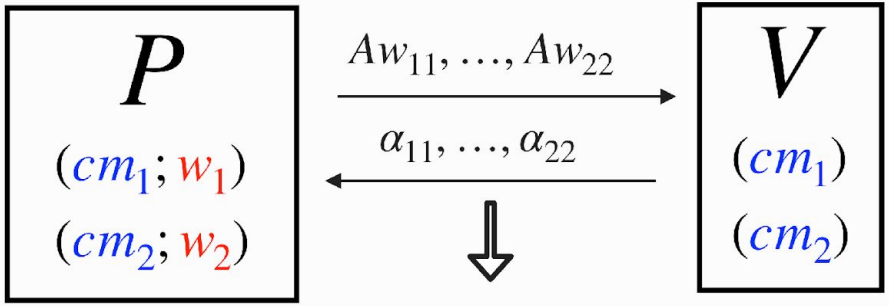
NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$

Solution (Latticefold)

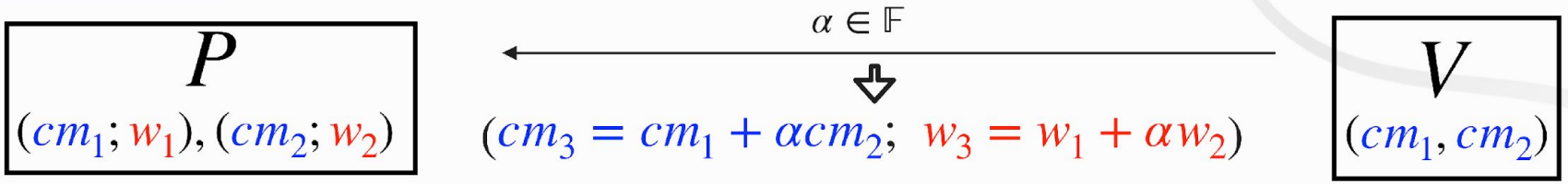


$$\begin{pmatrix} cm_3 = \alpha_{11} Aw_{11} + \ldots + \alpha_{22} Aw_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

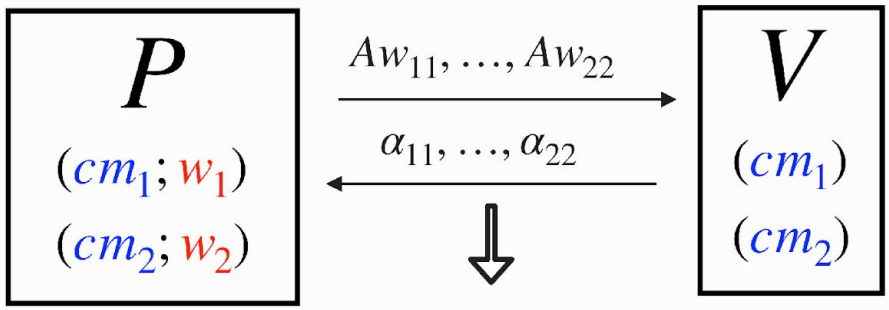
Call the w_{ij} chunks

NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



Solution (Latticefold)

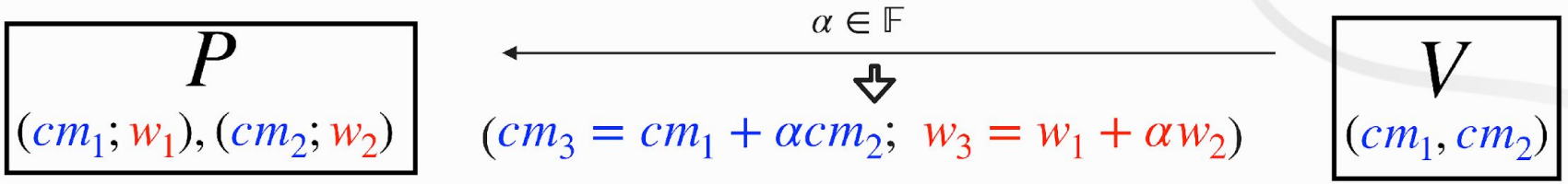
Called decomposition step

$$\begin{pmatrix} cm_3 = \alpha_{11} Aw_{11} + \ldots + \alpha_{22} Aw_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

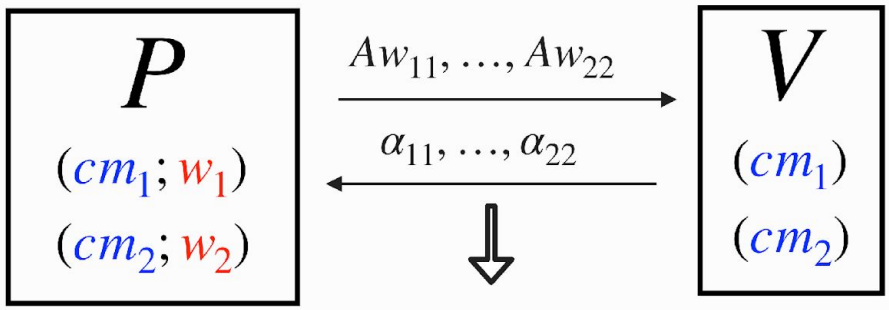
Call the w_{ij} chunks

NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\begin{pmatrix} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Solution (Latticefold)

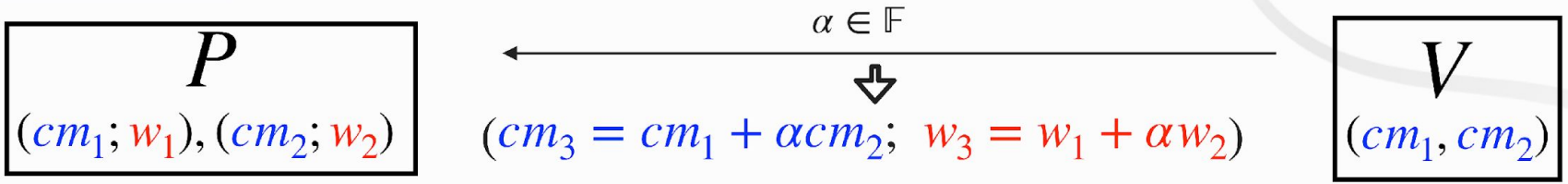
Called decomposition step

In LF, it requires splitting each w_i in many more than 2 chunks.

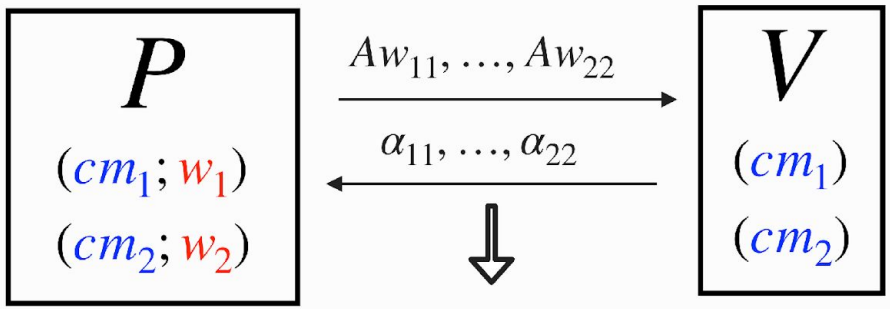
Call the w_{ij} chunks

NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\begin{pmatrix} cm_3 = \alpha_{11} Aw_{11} + \ldots + \alpha_{22} Aw_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Solution (Latticefold)

Called decomposition step

In LF, it requires splitting each w_i in many more than 2 chunks.

LF+, manages to make this step almost costless.

Call the w_{ij} chunks

NETHERMIND RESEARCH

Solving norm increases

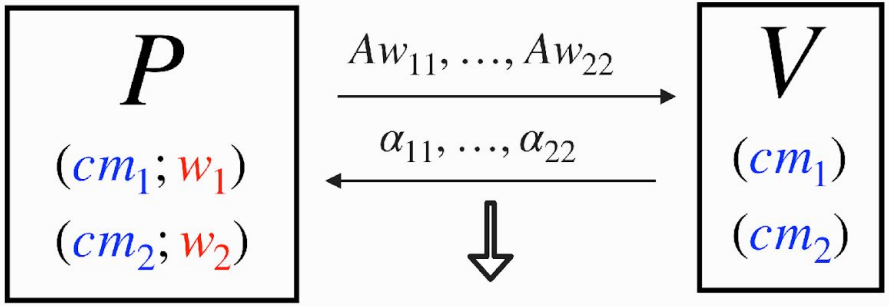
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\left(\begin{array}{c} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{array}\right)$$

Call the w_{ij} chunks

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

NETHERMIND RESEARCH

Solving norm increases

Configuration

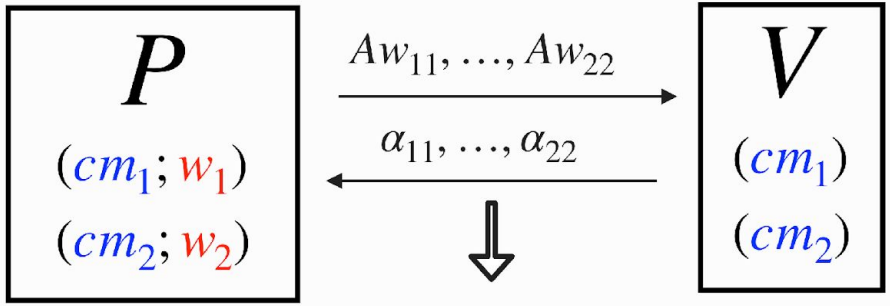
$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$

Experiments



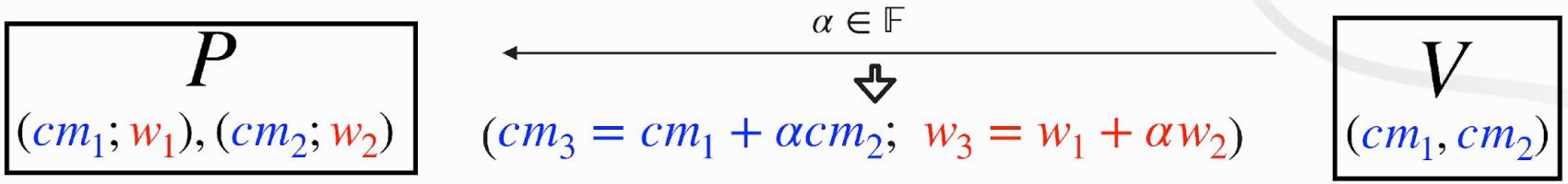
$$\begin{pmatrix} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Call the w_{ij} chunks

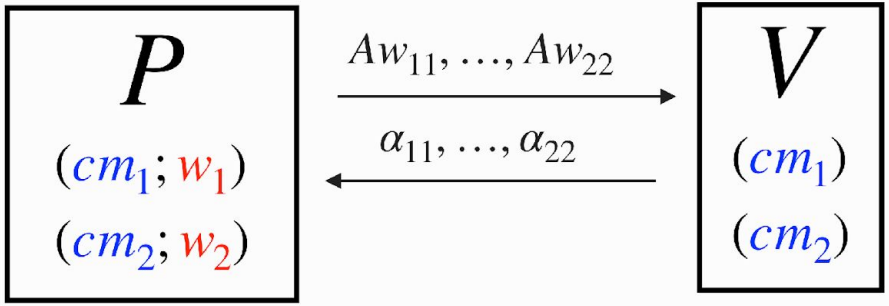
AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



Solution (Latticefold)

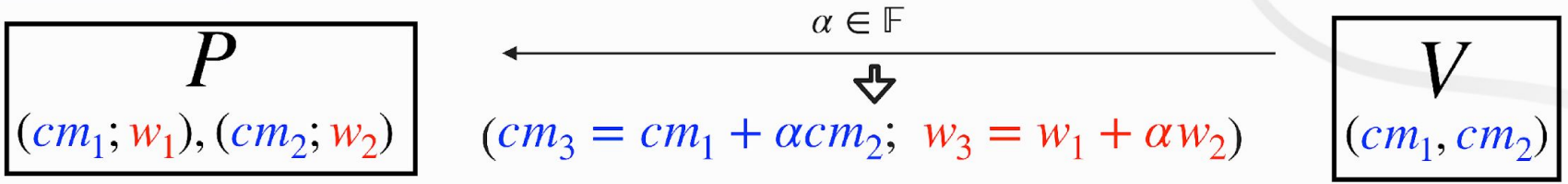
P writes $b^2 = B$ and

$$w_1 = w_{11} + w_{12}b$$

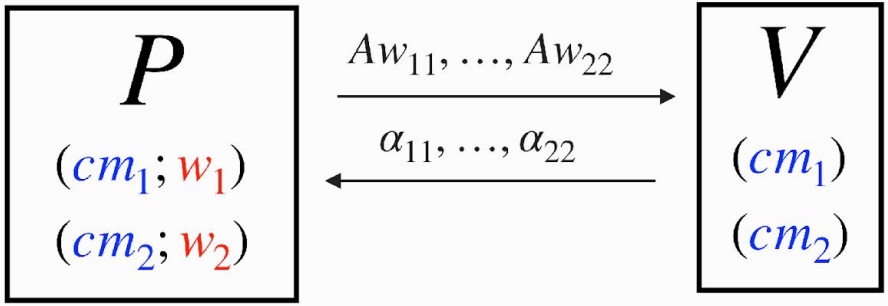
$$w_2 = w_{21} + w_{22}b$$

V sends $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ sampled in certain subset of $\mathcal{R}$ that guarantees

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



Solution (Latticefold)

P writes $b^2 = B$ and

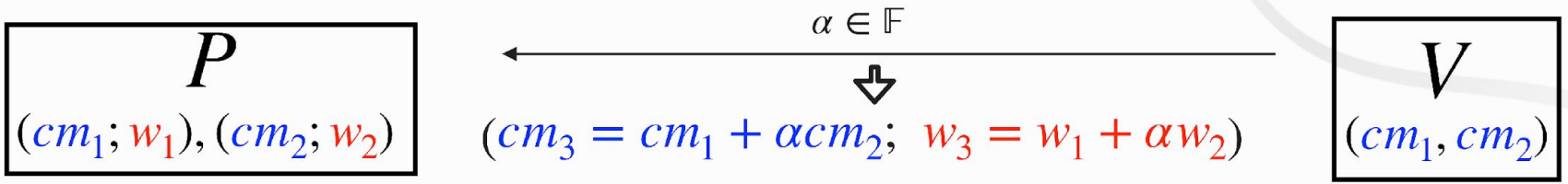
$$w_1 = w_{11} + w_{12}b$$

$$w_2 = w_{21} + w_{22}b$$

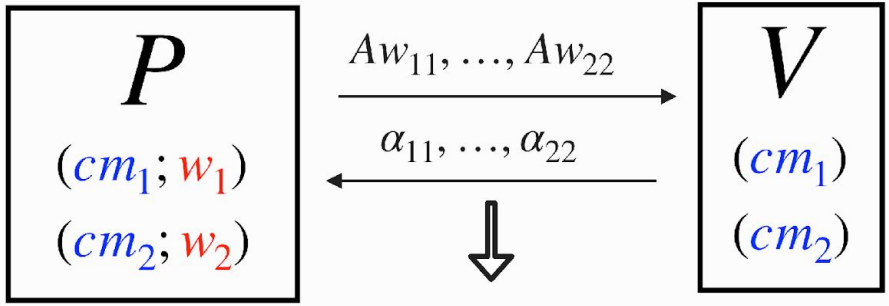
V sends $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ sampled in certain subset of $\mathcal{R}$ that guarantees

$$\|\alpha_{11}w_{11} + \ldots + \alpha_{22}w_{22}\| \leq B$$

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\left(\begin{array}{c} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{array}\right)$$

Solution (Latticefold)

P writes $b^2 = B$ and

$$w_1 = w_{11} + w_{12} b$$

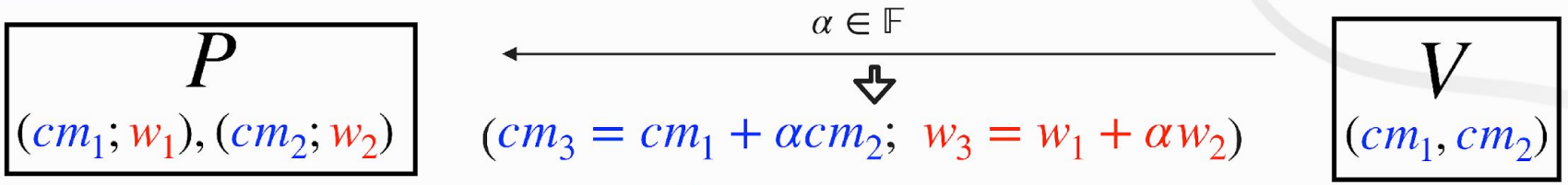
$$w_2 = w_{21} + w_{22} b$$

V sends $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ sampled in certain subset of $\mathcal{R}$ that guarantees

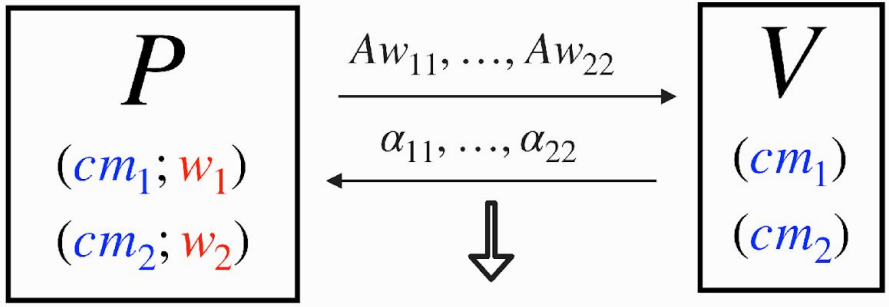
$$\|\alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22}\| \leq B$$

NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\begin{pmatrix} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Solution (Latticefold)

P writes $b^2 = B$ and

$$w_1 = w_{11} + w_{12} b$$

$$w_2 = w_{21} + w_{22} b$$

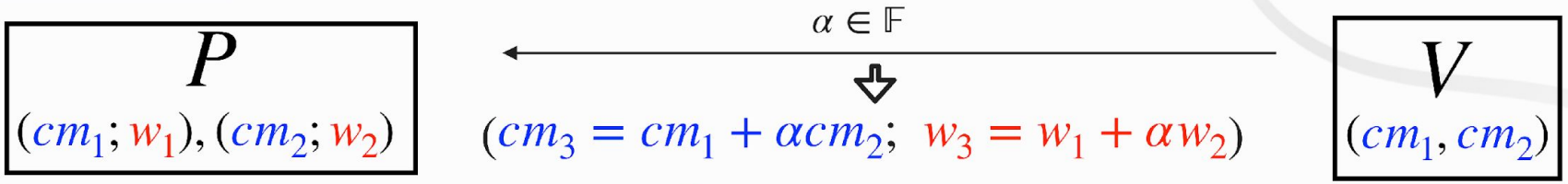
V sends $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ sampled in certain subset of $\mathcal{R}$ that guarantees

$$\|\alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22}\| \leq B$$

Call the w_{ij} chunks

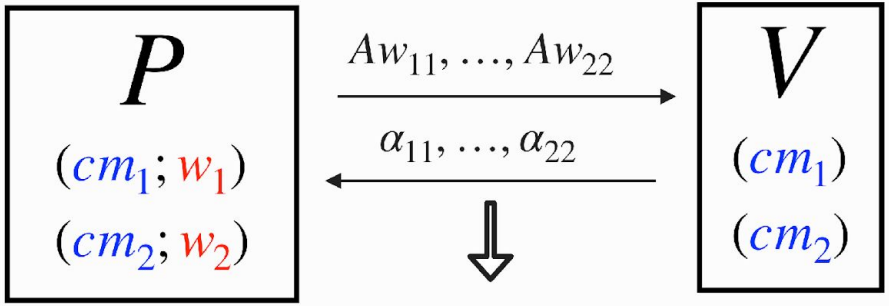
NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$

Solution (Latticefold)

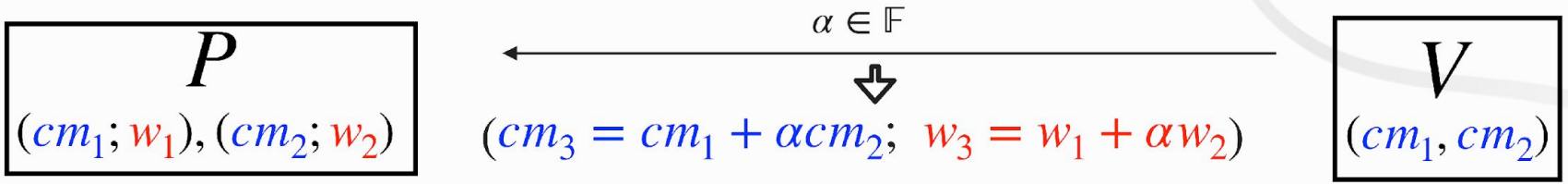


$$\begin{pmatrix} cm_3 = \alpha_{11} Aw_{11} + \ldots + \alpha_{22} Aw_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

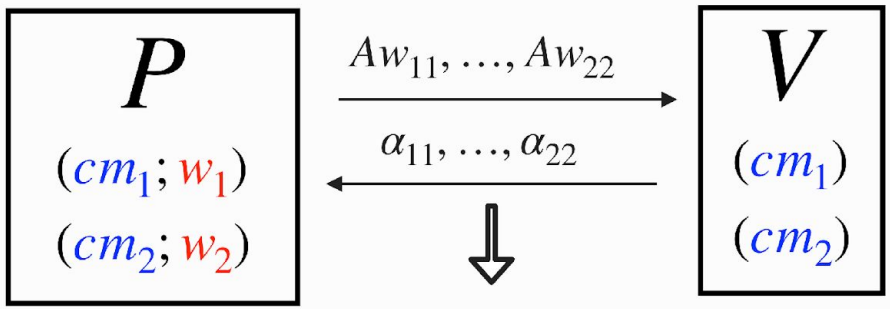
Call the w_{ij} chunks

NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



Solution (Latticefold)

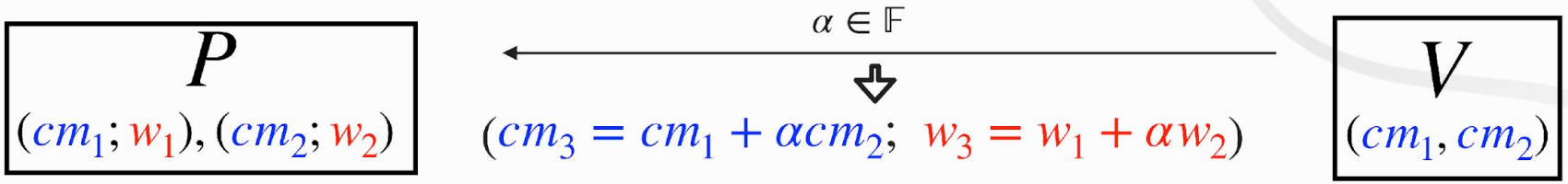
Called decomposition step

$$\begin{pmatrix} cm_3 = \alpha_{11} Aw_{11} + \ldots + \alpha_{22} Aw_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

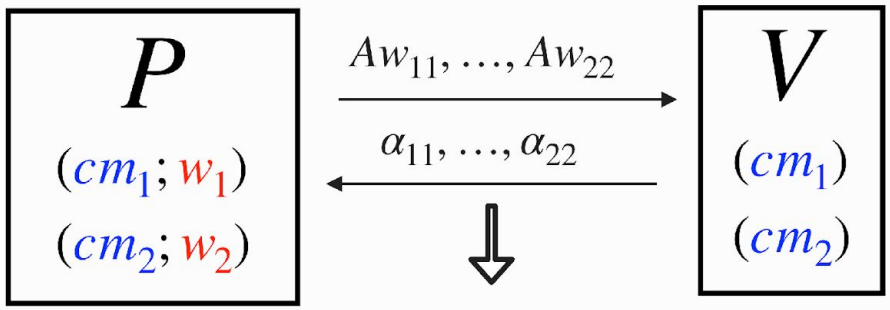
Call the w_{ij} chunks

NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\begin{pmatrix} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Solution (Latticefold)

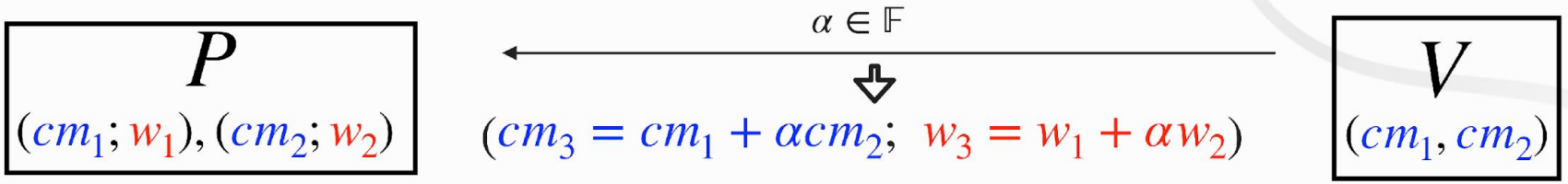
Called decomposition step

In LF, it requires splitting each w_i in many more than 2 chunks.

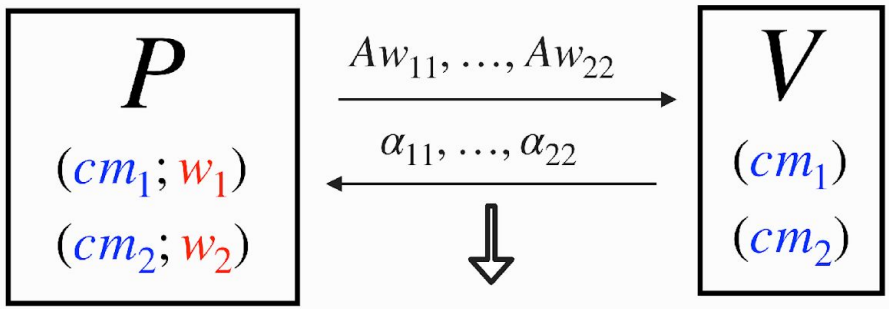
Call the w_{ij} chunks

NETHERMIND RESEARCH

Solving norm increases



Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\begin{pmatrix} cm_3 = \alpha_{11} Aw_{11} + \ldots + \alpha_{22} Aw_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Solution (Latticefold)

Called decomposition step

In LF, it requires splitting each w_i in many more than 2 chunks.

LF+, manages to make this step almost costless.

Call the w_{ij} chunks

NETHERMIND RESEARCH

Solving norm increases

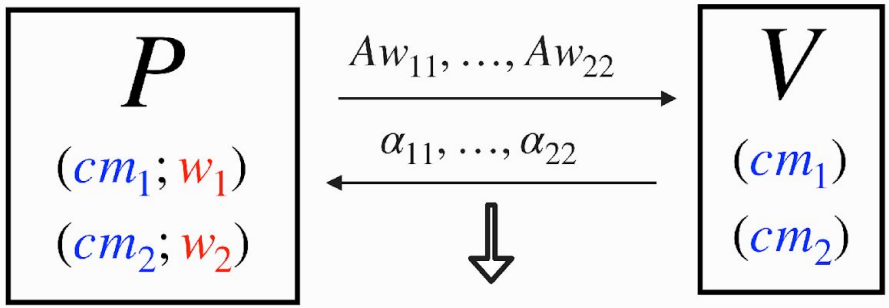
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\begin{pmatrix} cm_3 = \alpha_{11} Aw_{11} + \ldots + \alpha_{22} Aw_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Call the w_{ij} chunks

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

NETHERMIND RESEARCH

Solving norm increases

Configuration

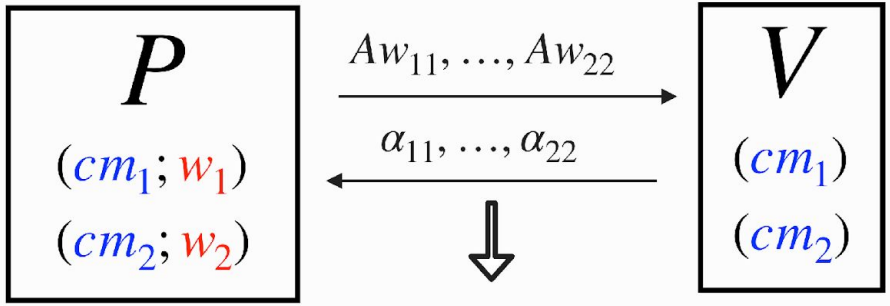
$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$

Experiments



$$\begin{pmatrix} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Call the w_{ij} chunks

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

NETHERMIND RESEARCH

Solving norm increases

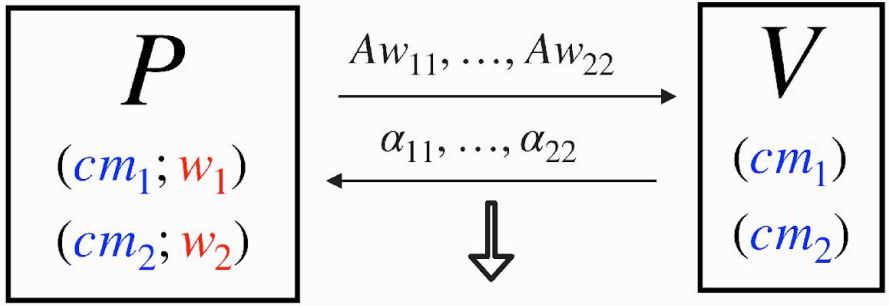
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\left(\begin{array}{c} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{array}\right)$$

Experiments

$|w_1|, |w_2| = 2^{16}$

Call the w_{ij} chunks

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

NETHERMIND RESEARCH

Solving norm increases

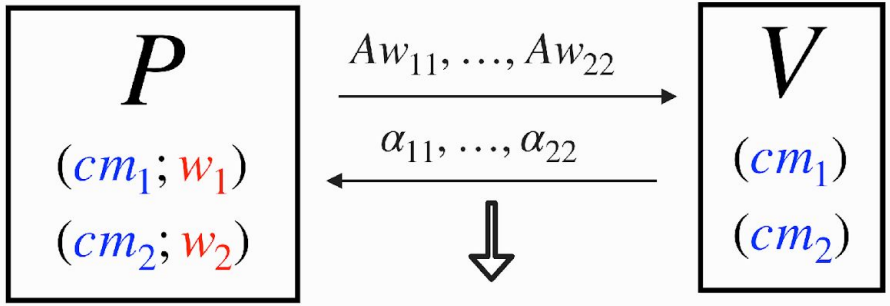
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\left(\begin{array}{c} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{array}\right)$$

Experiments

$|w_1|, |w_2| = 2^{16}$

Use 8 chunks per w_i

Call the w_{ij} chunks

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

NETHERMIND RESEARCH

Solving norm increases

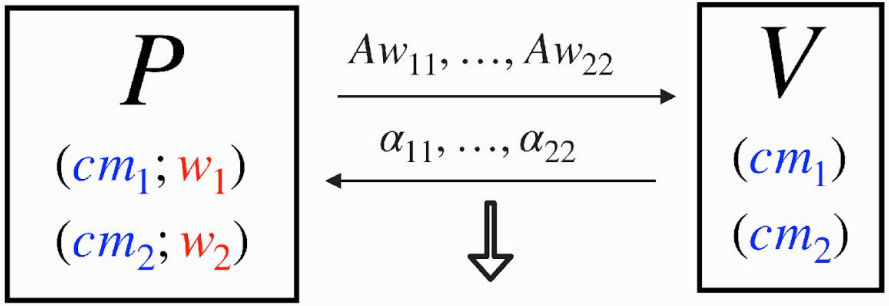
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\left(\begin{array}{c} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{array}\right)$$

Experiments

$|w_1|, |w_2| = 2^{16}$

Use 8 chunks per w_i

LF cost: 3s

Call the w_{ij} chunks

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

NETHERMIND RESEARCH

Solving norm increases

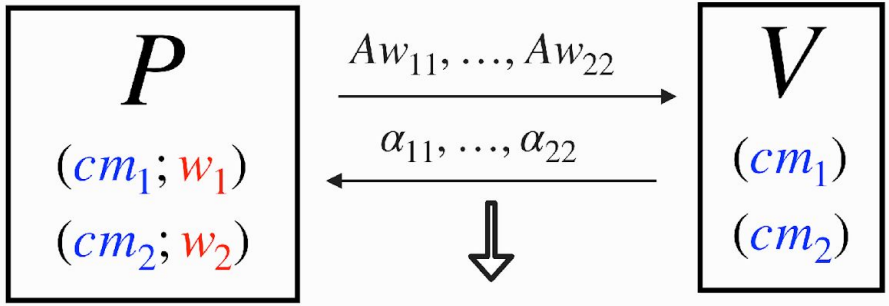
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\left(\begin{array}{c} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{array}\right)$$

Experiments

$|w_1|, |w_2| = 2^{16}$

Use 8 chunks per w_i

LF cost: 3s

LF+ needs only 2 chunks in total

Call the w_{ij} chunks

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

NETHERMIND RESEARCH

Solving norm increases

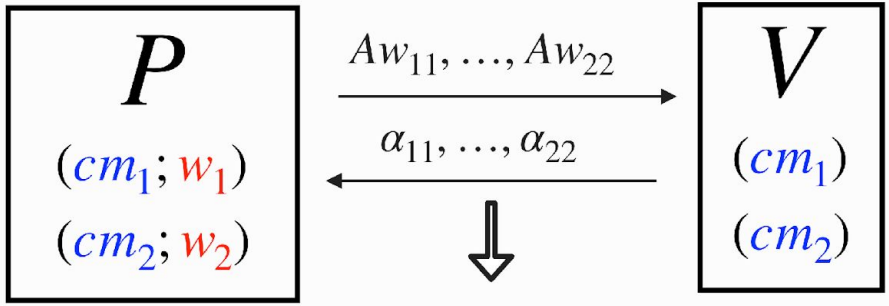
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\begin{pmatrix} cm_3 = \alpha_{11} A w_{11} + \ldots + \alpha_{22} A w_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Experiments

$|w_1|, |w_2| = 2^{16}$

Use 8 chunks per w_i

LF cost: 3s

LF+ needs only 2 chunks in total

LF+ expected cost: 0.4s

Call the w_{ij} chunks

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

NETHERMIND RESEARCH

Solving norm increases

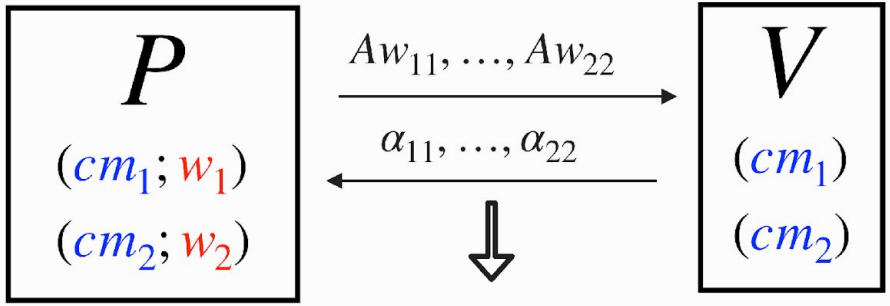
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Maybe $\|w_1 + \alpha w_2\| > B$



$$\begin{pmatrix} cm_3 = \alpha_{11} Aw_{11} + \ldots + \alpha_{22} Aw_{22}; \\ w_3 = \alpha_{11} w_{11} + \ldots + \alpha_{22} w_{22} \end{pmatrix}$$

Experiments

$|w_1|, |w_2| = 2^{16}$

Use 8 chunks per w_i

LF cost: 3s

LF+ needs only 2 chunks in total

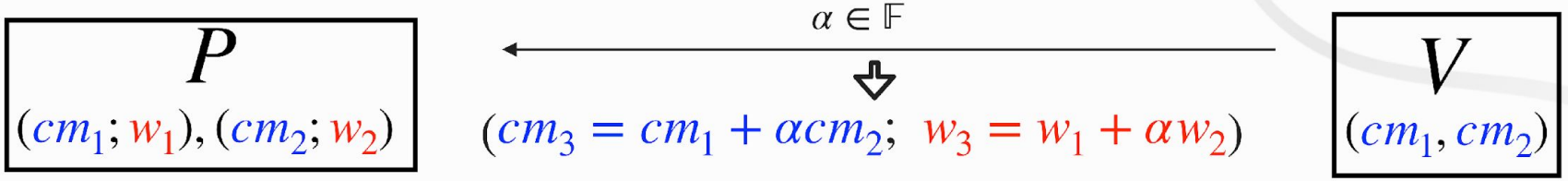
LF+ expected cost: 0.4s

Call the w_{ij} chunks

NETHERMIND RESEARCH

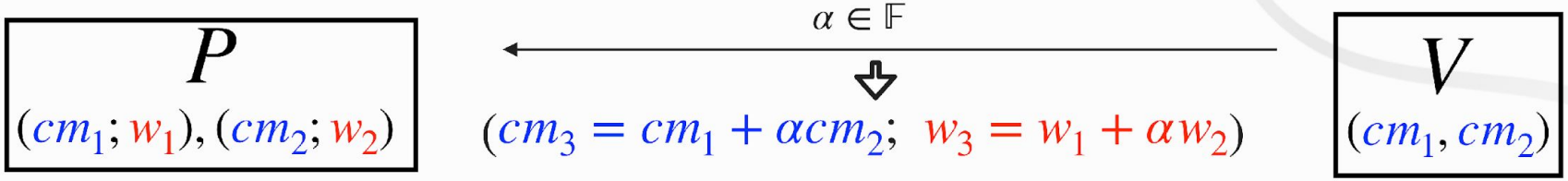
AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds



NETHERMIND RESEARCH

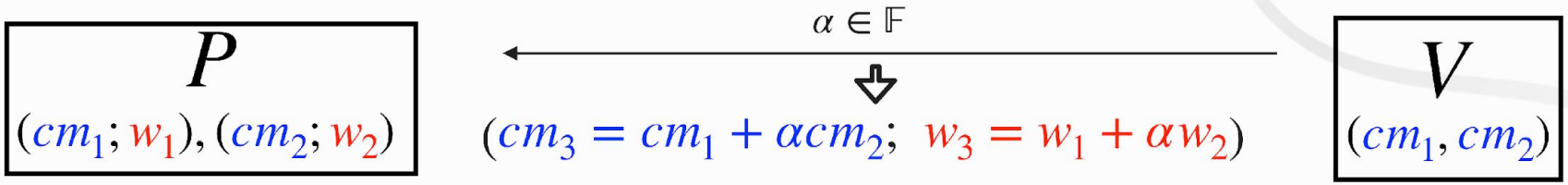
Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

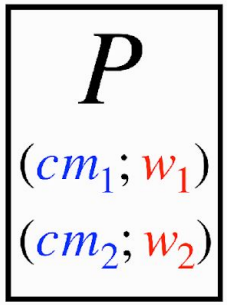
NETHERMIND RESEARCH

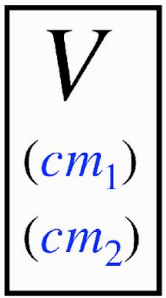
Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

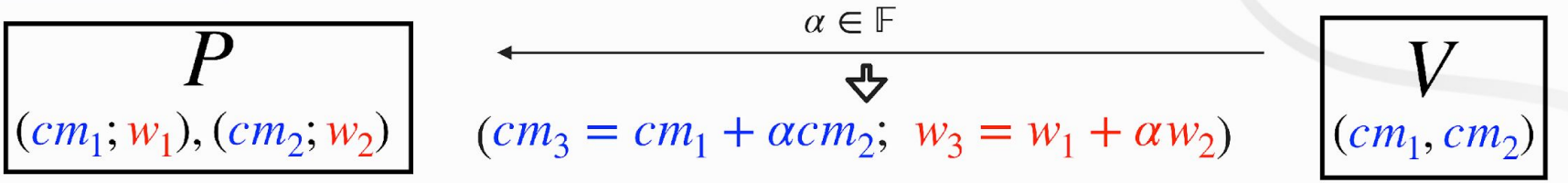
Solution (Latticefold)



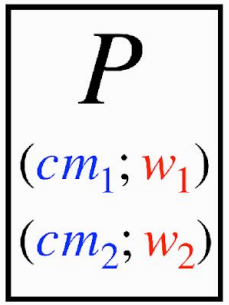


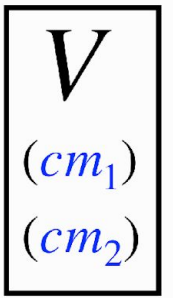
NETHERMIND RESEARCH

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

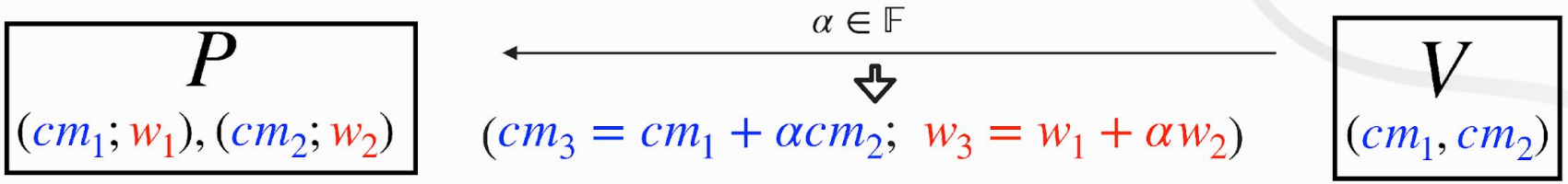




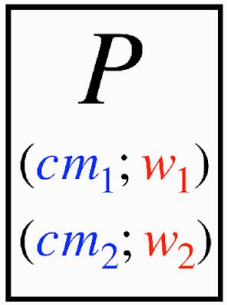
Solution (Latticefold)

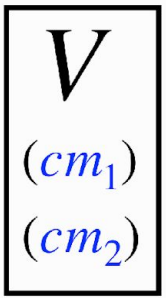
Replace $\|w_i\| < B$ by

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$





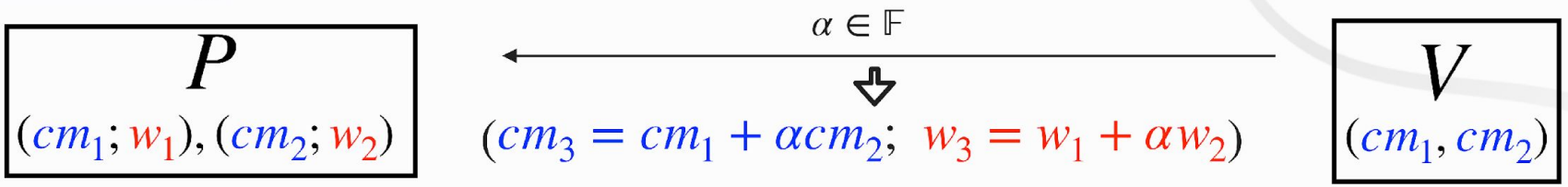
Solution (Latticefold)

Replace $\|w_i\| < B$ by

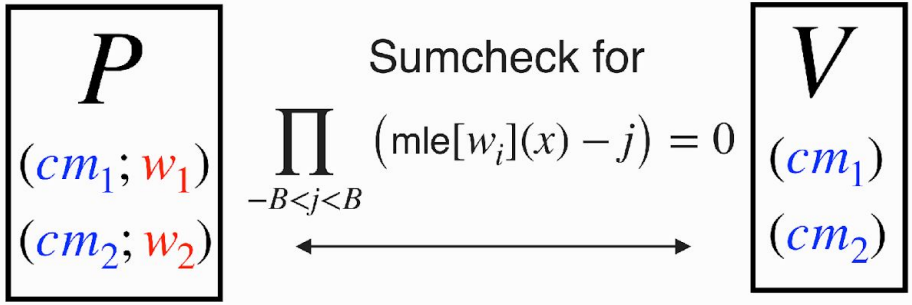
$\Pi_{-B<j<B} \left(\text{mle}[w_i](x) - j\right) = 0 \quad \forall\ x \in \{0,1\}^{\log(m)}$

NETHERMIND RESEARCH

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Solution (Latticefold)

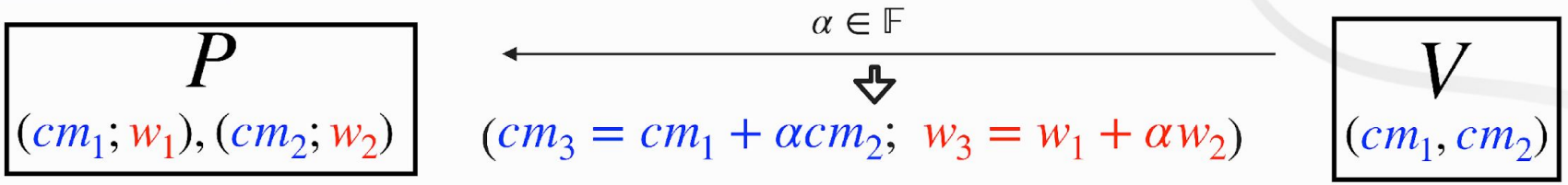
Replace $\|w_i\| < B$ by

$\Pi_{-B<j<B} \left(\text{mle}[w_i](x) - j\right) = 0 \quad \forall\ x \in \{0,1\}^{\log(m)}$

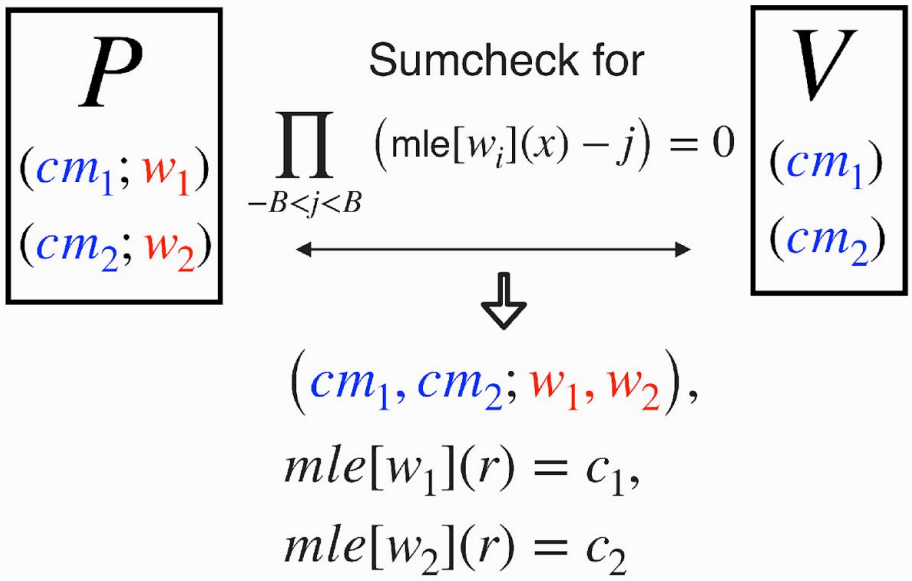
Run sumcheck and reduce it to a multilinear polynomial evaluation claim.

NETHERMIND RESEARCH

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Solution (Latticefold)

Replace $\|w_i\| < B$ by

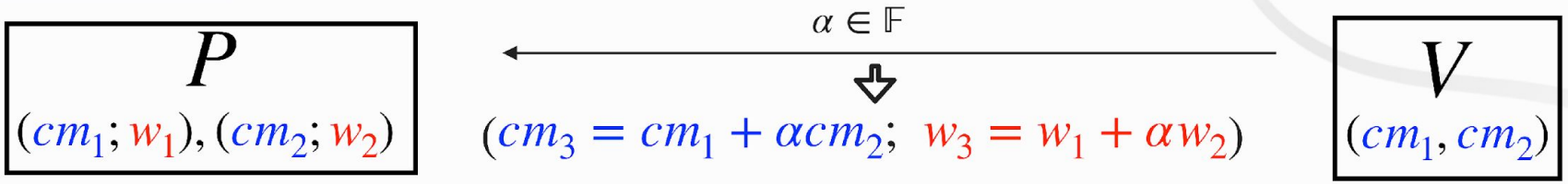
$\Pi_{-B<j<B} (\text{mle}[w_i](x) - j) = 0 \quad \forall\, x \in \{0,1\}^{\log(m)}$

Run sumcheck and reduce it to a multilinear polynomial evaluation claim.

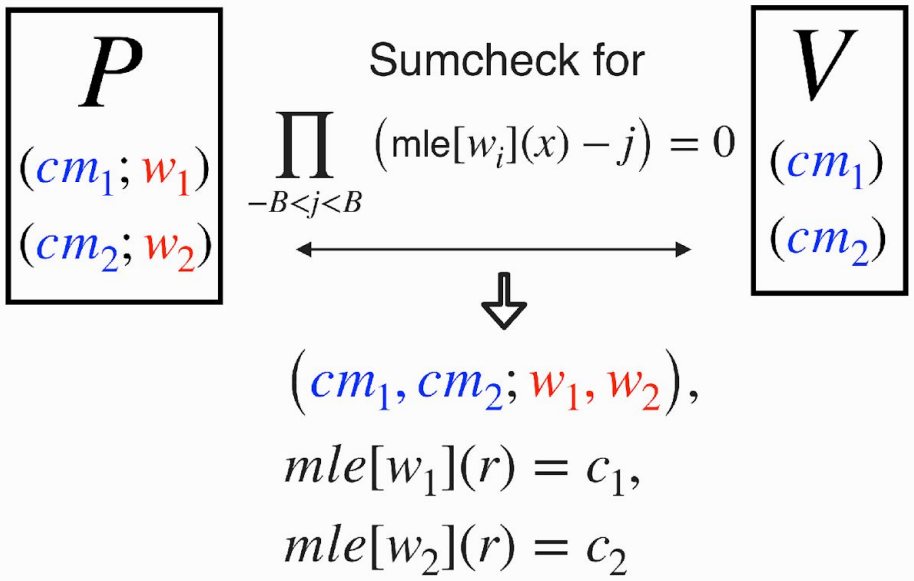
Add this claim to the folded relation.

NETHERMIND RESEARCH

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Solution (Latticefold)

Replace $\|w_i\| < B$ by

$\Pi_{-B<j<B} (\text{mle}[w_i](x) - j) = 0 \quad \forall\ x \in \{0,1\}^{\log(m)}$

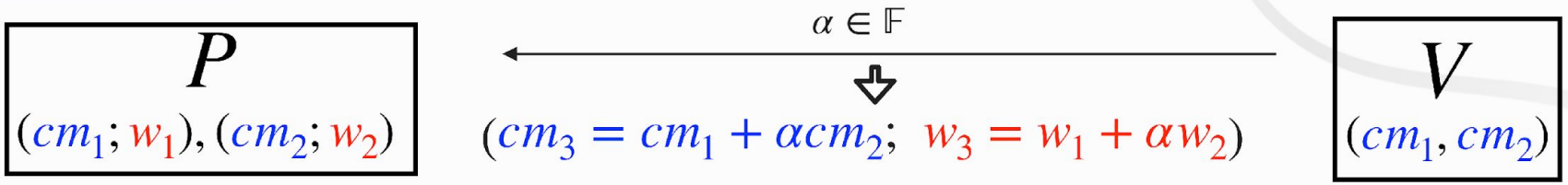
Run sumcheck and reduce it to a multilinear polynomial evaluation claim.

Add this claim to the folded relation.

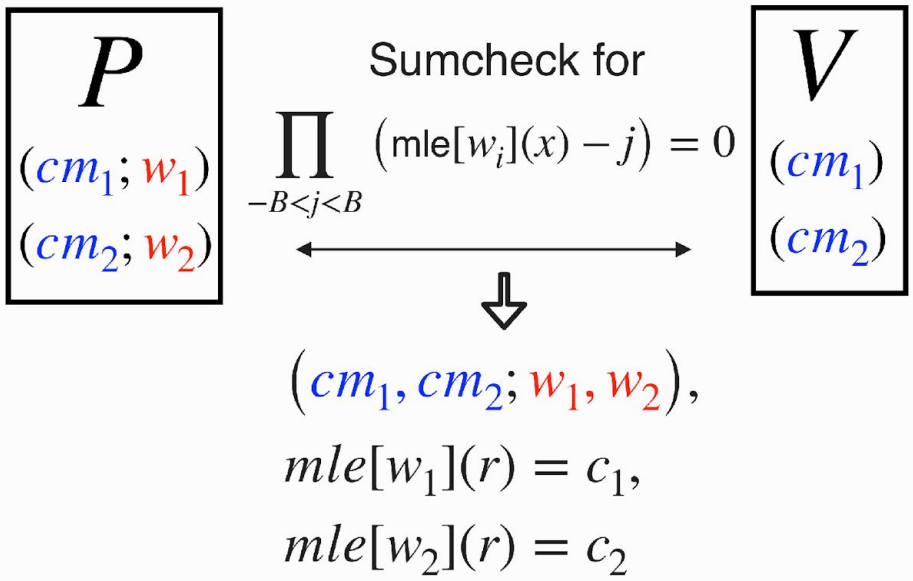
In LF, there's a sumcheck per chunk w_{ij}

NETHERMIND RESEARCH

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Solution (Latticefold)

Replace $\|w_i\| < B$ by

$\Pi_{-B<j<B} (\text{mle}[w_i](x) - j) = 0 \quad \forall\ x \in \{0,1\}^{\log(m)}$

Run sumcheck and reduce it to a multilinear polynomial evaluation claim.

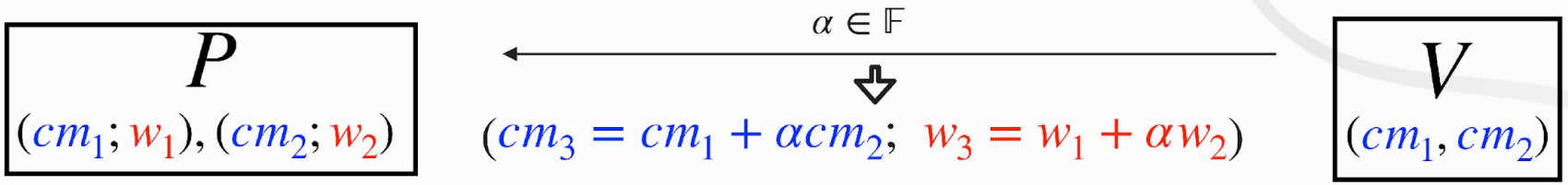
Add this claim to the folded relation.

In LF, there's a sumcheck per chunk w_{ij}

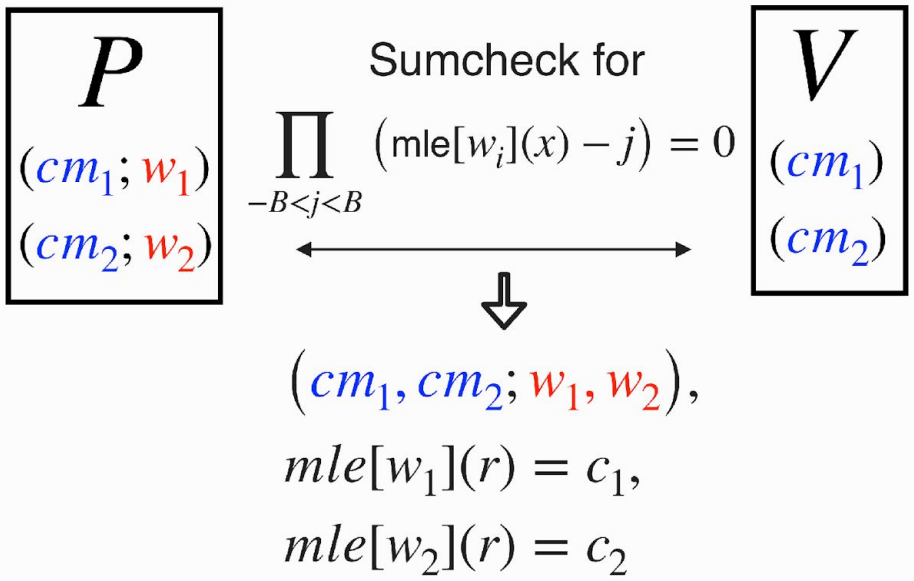
(These are batched)

NETHERMIND RESEARCH

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Solution (Latticefold)

Replace $\|w_i\| < B$ by

$\Pi_{-B<j<B} (\text{mle}[w_i](x) - j) = 0 \quad \forall\ x \in \{0,1\}^{\log(m)}$

Run sumcheck and reduce it to a multilinear polynomial evaluation claim.

Add this claim to the folded relation.

In LF, there's a sumcheck per chunk w_{ij}

(These are batched)

And B is replaced by b

NETHERMIND RESEARCH

Solving norm bounds

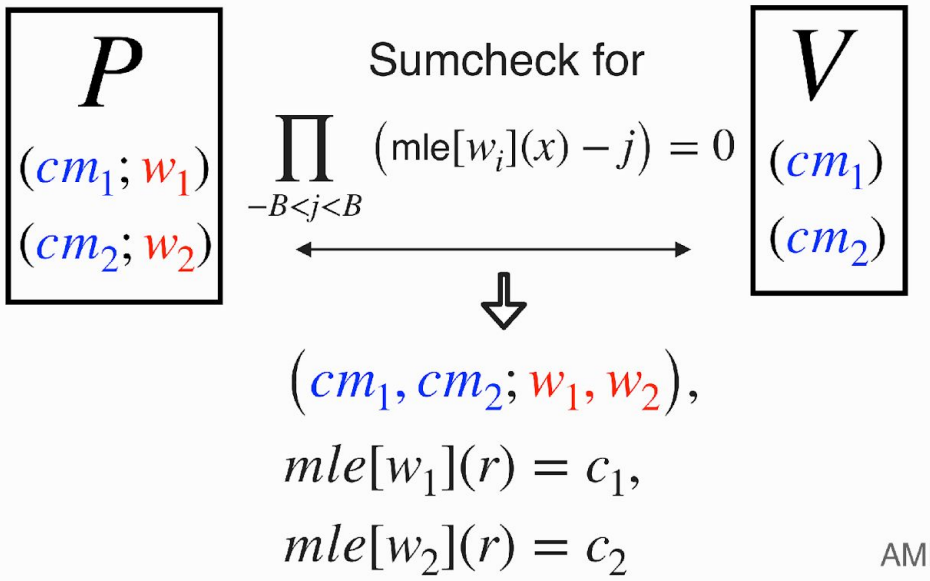
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds

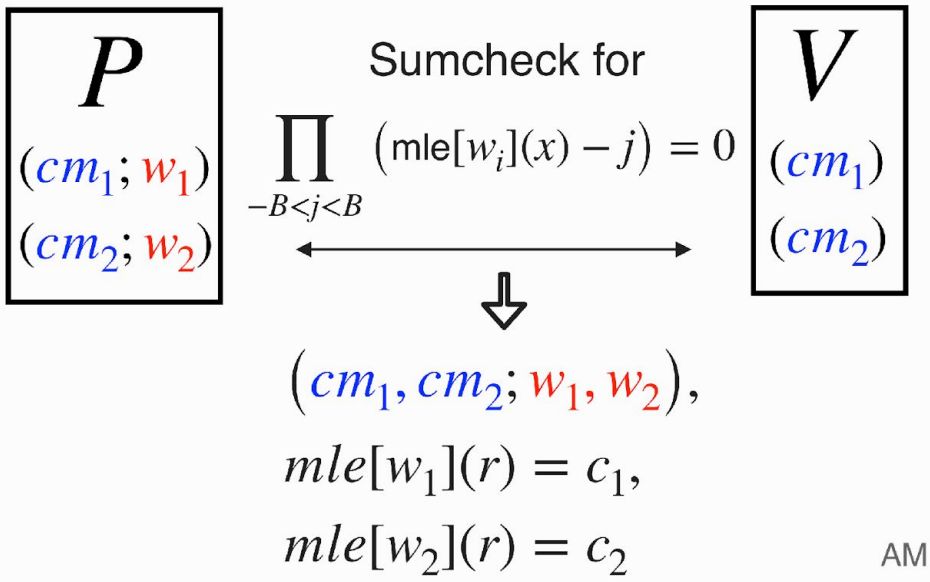
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm, \|w\| \leq B\}$



Experiments

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds

Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm, \|w\| \leq B\}$

P

$(cm_1; w_1)$

$(cm_2; w_2)$

Sumcheck for

$$\prod_{-B<j<B} \left(\text{mle}[w_i](x) - j\right) = 0$$

V

(cm_1)

(cm_2)

$$\left(cm_1, cm_2; w_1, w_2\right),$$

$$mle[w_1](r) = c_1,$$

$$mle[w_2](r) = c_2$$

Experiments

$|w_1|, |w_2| = 2^{16}$

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds

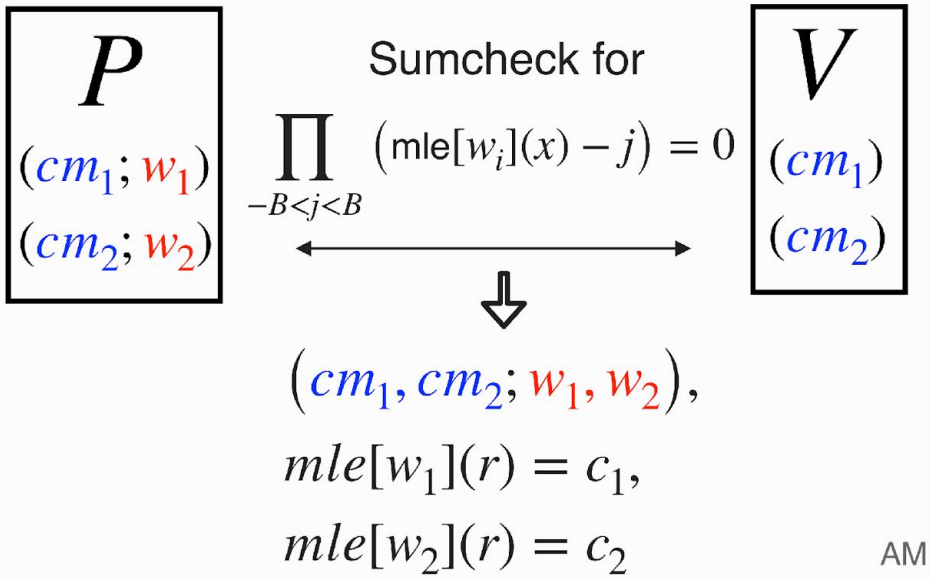
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Experiments

$|w_1|, |w_2| = 2^{16}$

When $B = 2$, one single grand product sumcheck costs 0.18s

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds

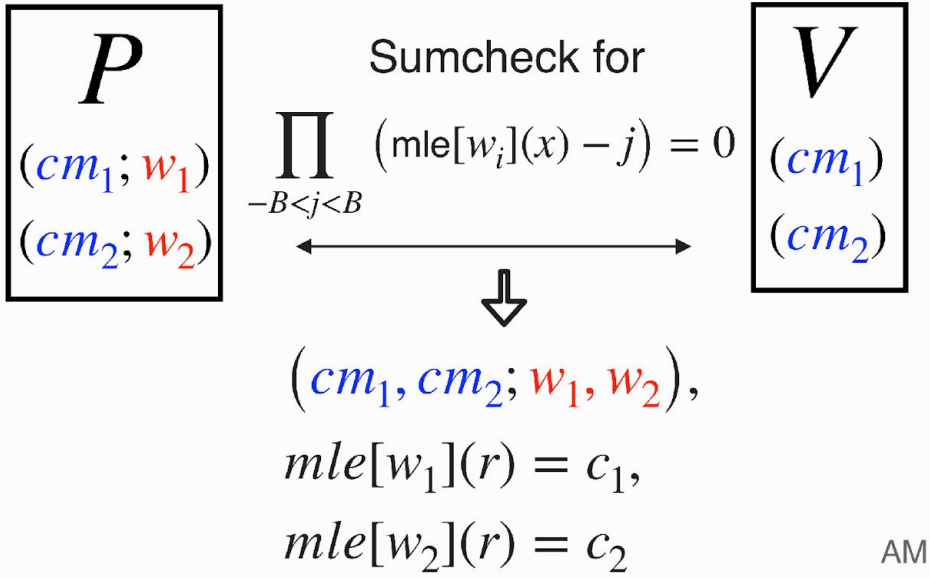
Configuration

$\mathbb{F}_q$ = Goldilocks field (64 bits), $q \approx 2^{64}$.

$\mathscr{R} = \mathbb{F}_q[X]/(X^{24} - X^{12} + 1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

Set $\kappa = 10$ and $B = 2^8$.

Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm, \|w\| \leq B\}$



Experiments

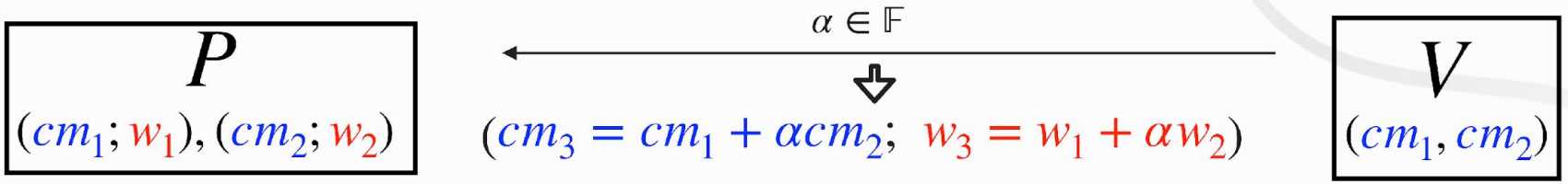
$|w_1|, |w_2| = 2^{16}$

When $B = 2$, one single grand product sumcheck costs 0.18s

LF performs one sumcheck per chunk, so total cost is 3s

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

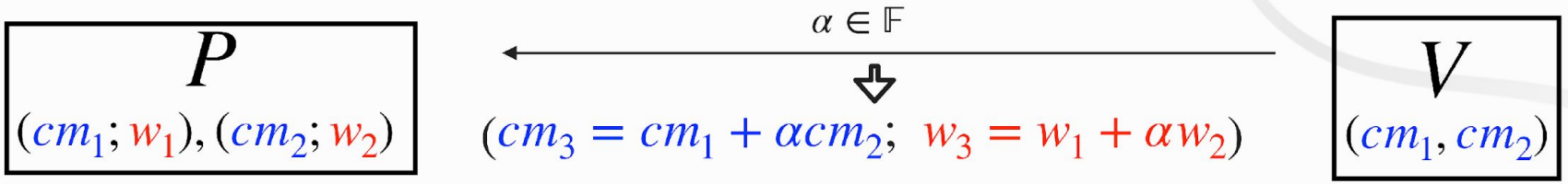
Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

Solution (Latticefold+ w/o double commits)

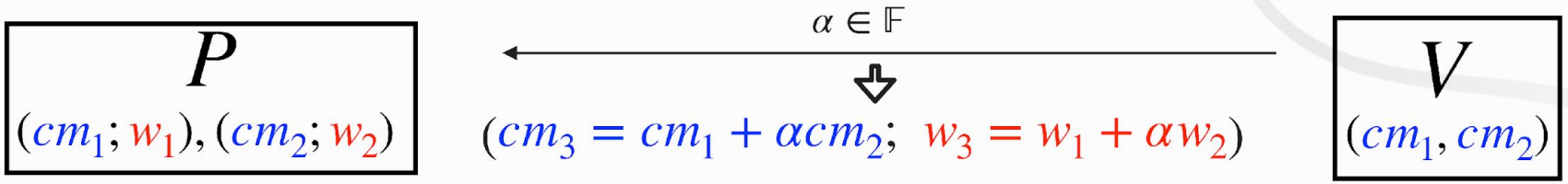
Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

Solution (Latticefold+ w/o double commits)

Solving norm bounds

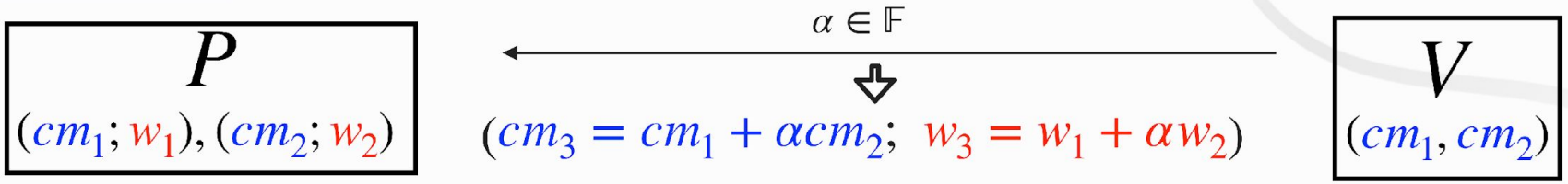


Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

Solution (Latticefold+ w/o double commits)

Commit to $X^{\text{coefficients of } w_1, w_2}$

Solving norm bounds



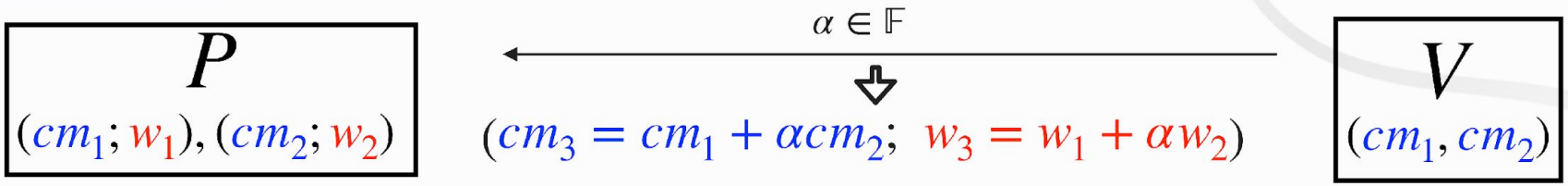
Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

Solution (Latticefold+ w/o double commits)

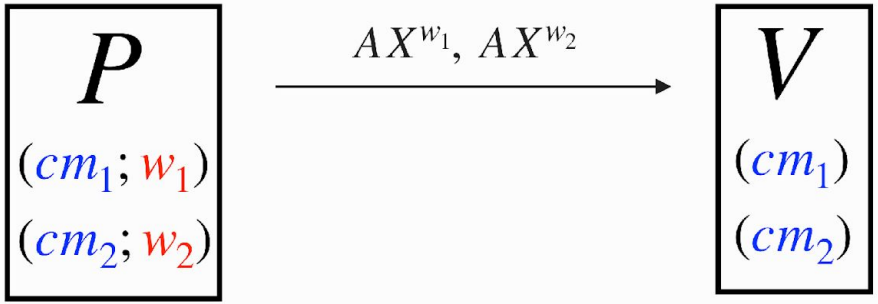
Commit to $X^{\text{coefficients of } w_1, w_2}$

Notation: $AX^{w_i} \in \mathcal{R}^{\kappa \times \deg(f)}$

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

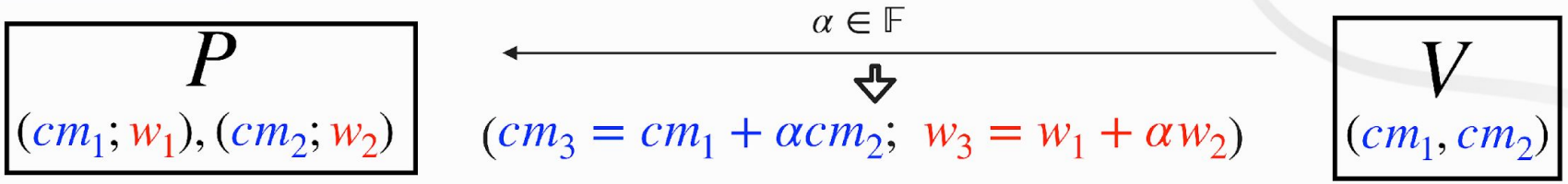


Solution (Latticefold+ w/o double commits)

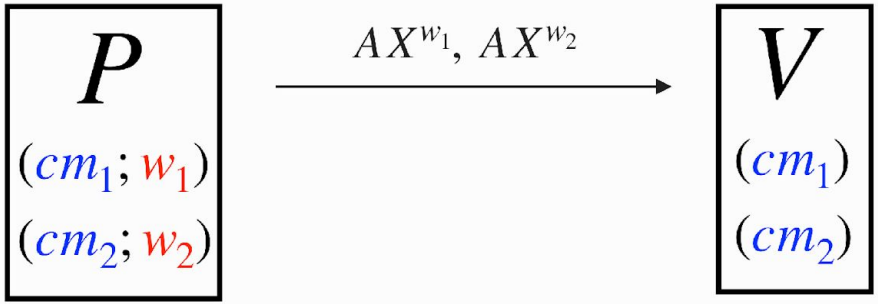
Commit to Xcoefficients of w_1, w_2

Notation: $AX^{w_i} \in \mathcal{R}^{\kappa \times \deg(f)}$

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



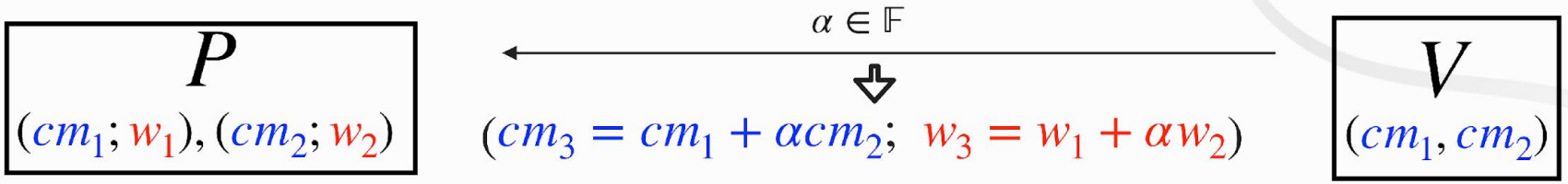
Solution (Latticefold+ w/o double commits)

Commit to Xcoefficients of w_1, w_2

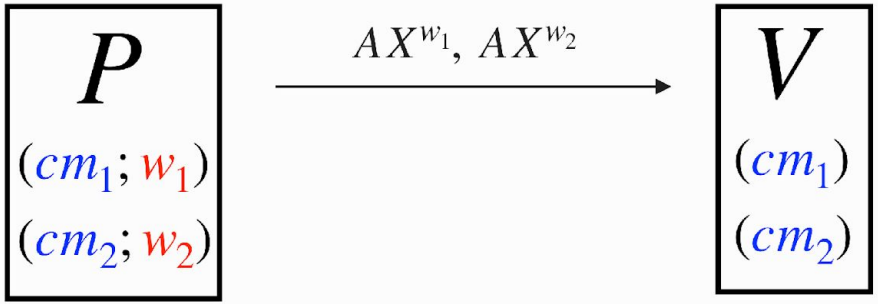
Notation: $AX^{w_i} \in \mathcal{R}^{\kappa \times \deg(f)}$

Fast:

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Solution (Latticefold+ w/o double commits)

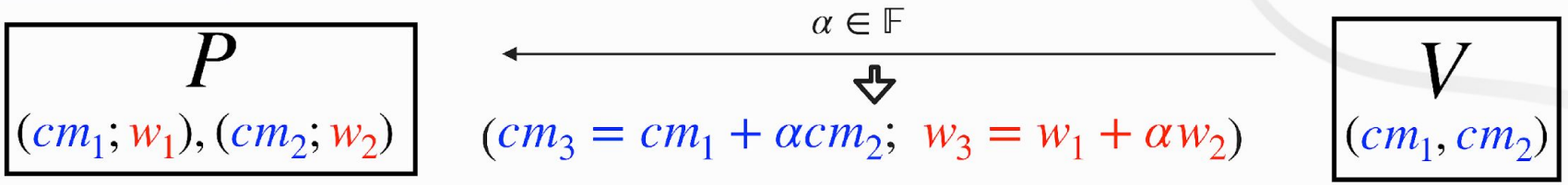
Commit to Xcoefficients of w_1, w_2

Notation: $AX^{w_i} \in \mathcal{R}^{\kappa \times \deg(f)}$

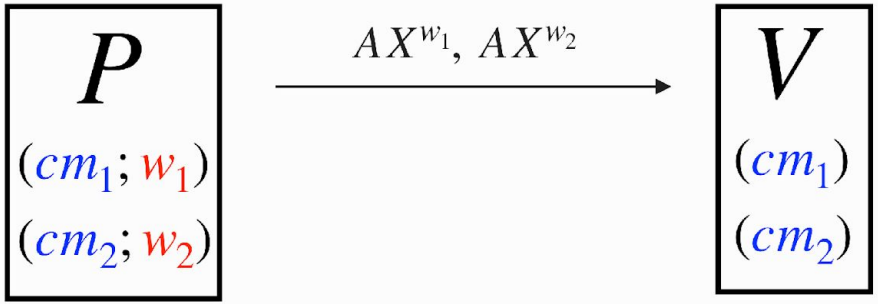
Fast:

- Only multiplication by monomials

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Solution (Latticefold+ w/o double commits)

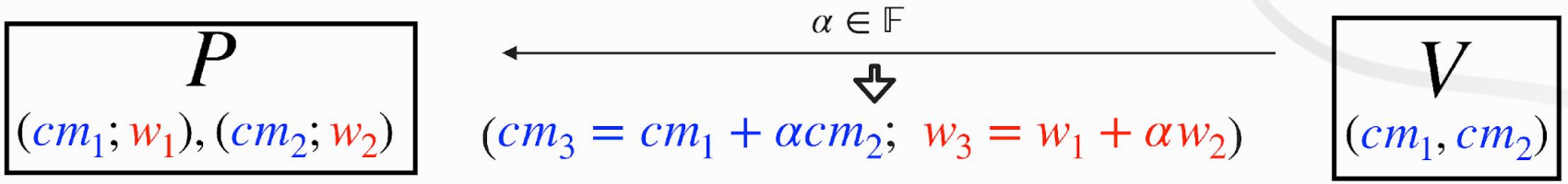
Commit to Xcoefficients of w_1, w_2

Notation: $AX^{w_i} \in \mathcal{R}^{\kappa \times \deg(f)}$

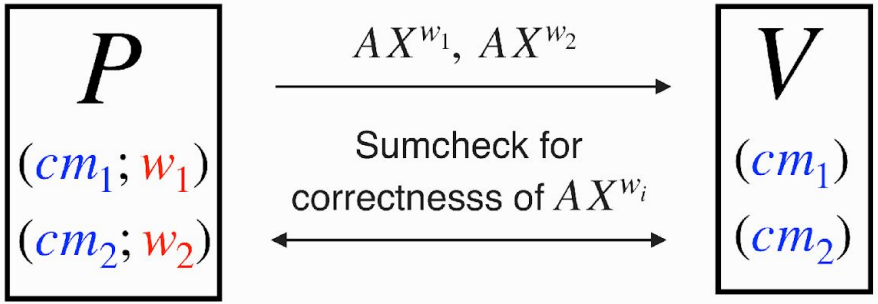
Fast:

- Only multiplication by monomials
- Low norm -> allows using small κ

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Solution (Latticefold+ w/o double commits)

Commit to Xcoefficients of w_1, w_2

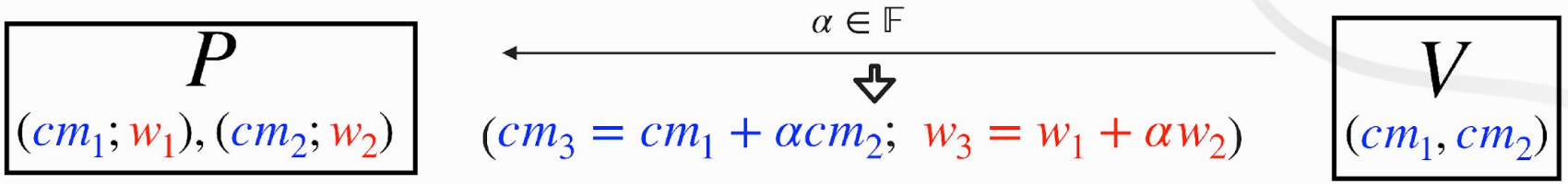
Notation: $AX^{w_i} \in \mathcal{R}^{\kappa \times \deg(f)}$

Fast:

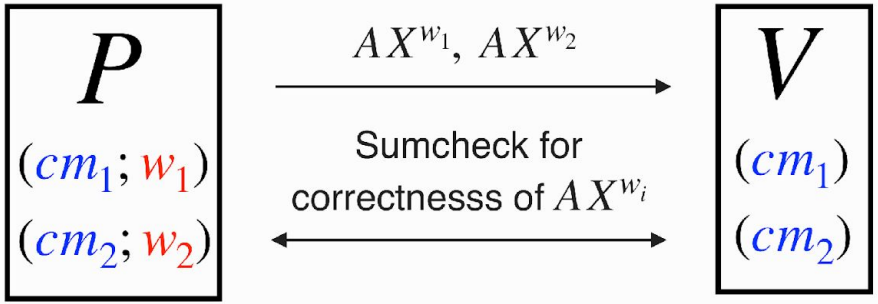
- Only multiplication by monomials
- Low norm -> allows using small κ

Sumcheck of correctness of AX^{w_i}

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Solution (Latticefold+ w/o double commits)

Commit to Xcoefficients of w_1, w_2

Notation: $AX^{w_i} \in \mathcal{R}^{\kappa \times \deg(f)}$

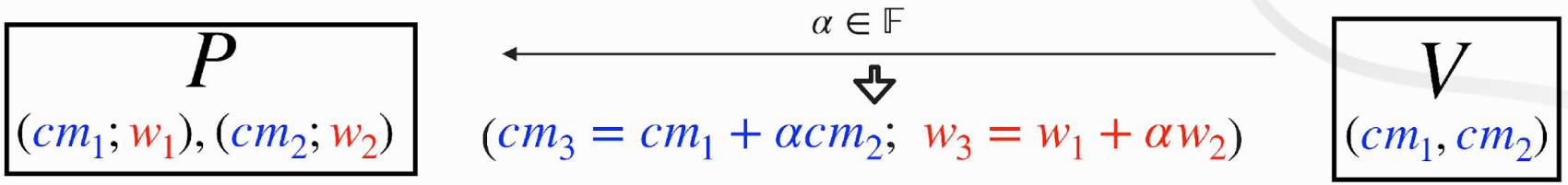
Fast:

- Only multiplication by monomials
- Low norm -> allows using small κ

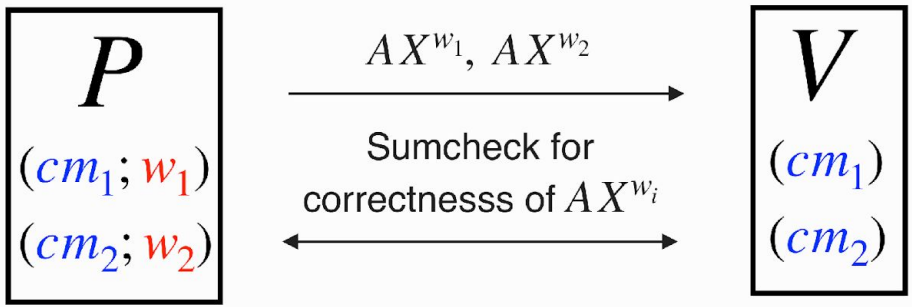
Sumcheck of correctness of AX^{w_i}

= $\deg(d)$ sum checks over $\mathbb{F}_q$

Solving norm bounds

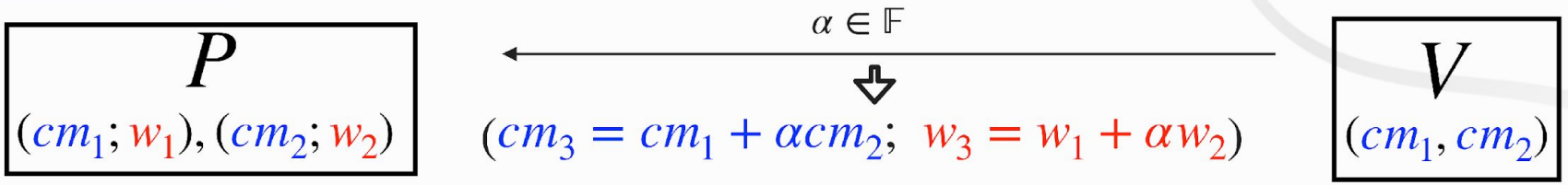


Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

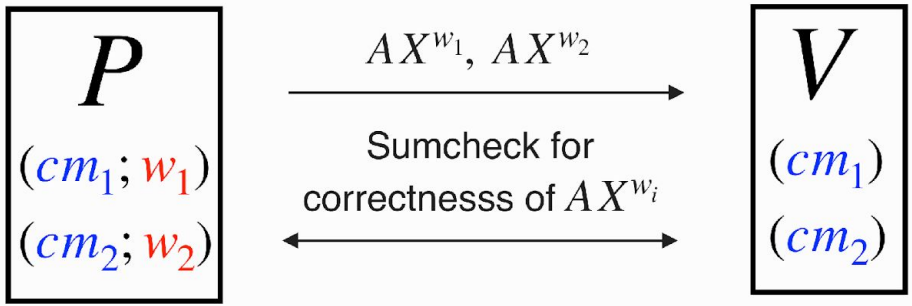


Solution (Latticefold+ w/o double commits)

Solving norm bounds



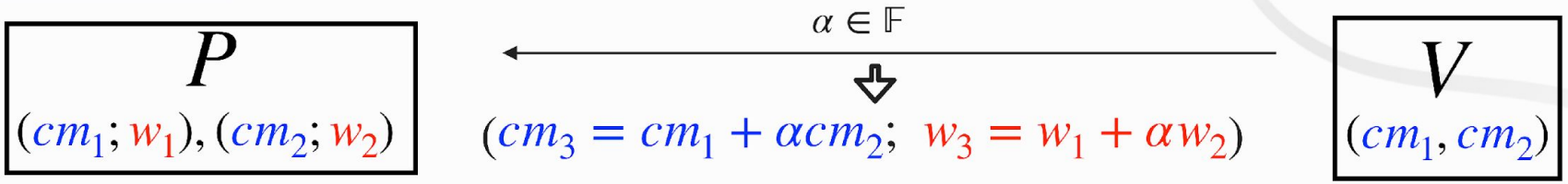
Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



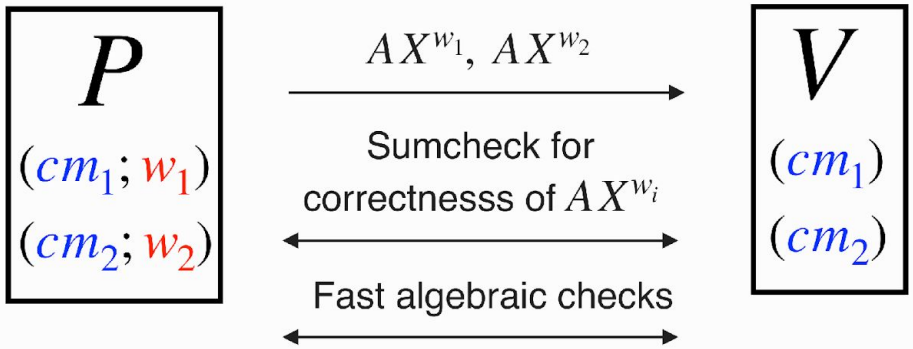
Solution (Latticefold+ w/o double commits)

Once AX^{w_1}, AX^{w_2} are committed,

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

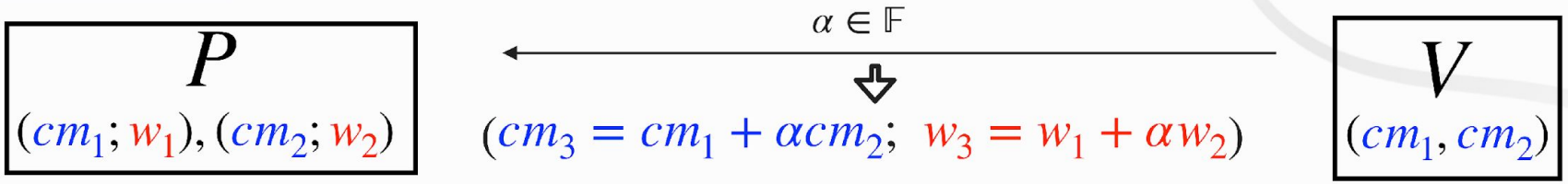


Solution (Latticefold+ w/o double commits)

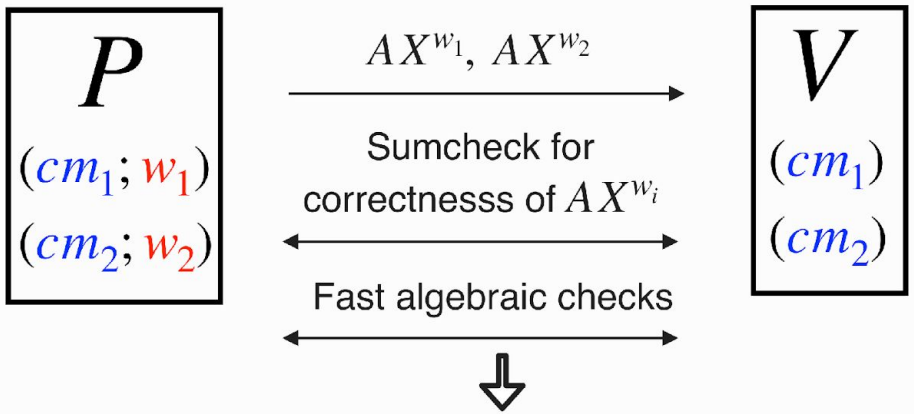
Once AX^{w_1}, AX^{w_2} are committed,

$\|w_i\| \leq B$ can be ensured with a simple algebraic check

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



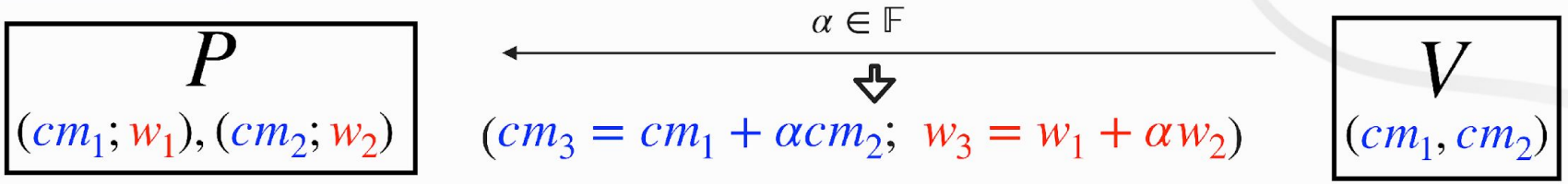
Claims about commitments, norm bounds and evaluations of multilinear polynomials

Solution (Latticefold+ w/o double commits)

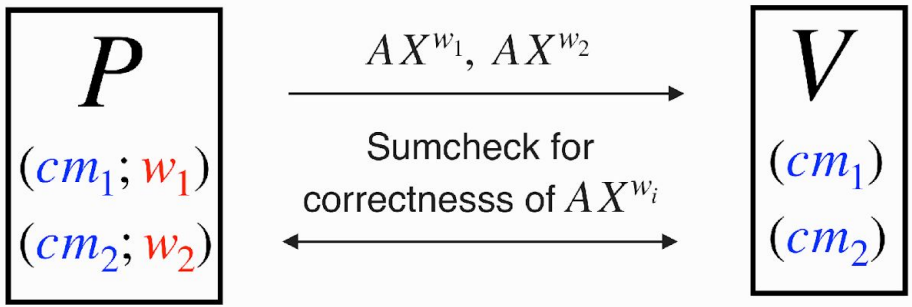
Once AX^{w_1}, AX^{w_2} are committed,

$\|w_i\| \leq B$ can be ensured with a simple algebraic check

Solving norm bounds

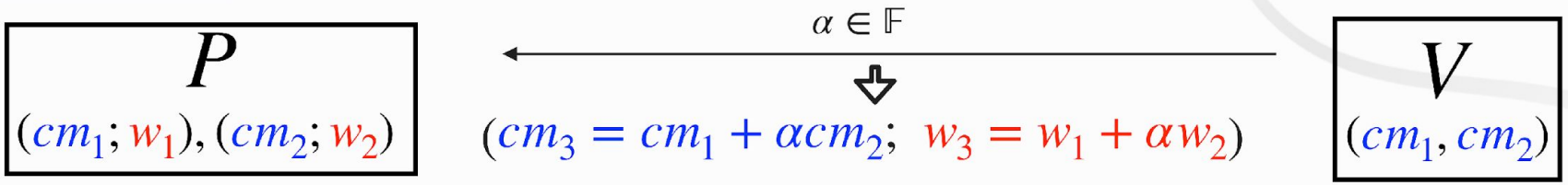


Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

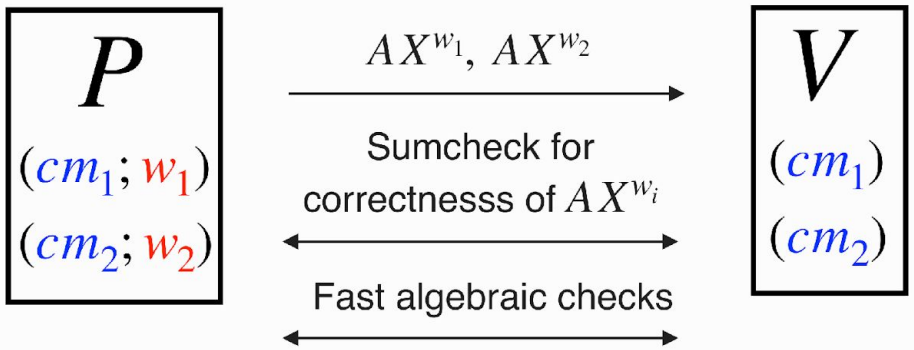


AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds

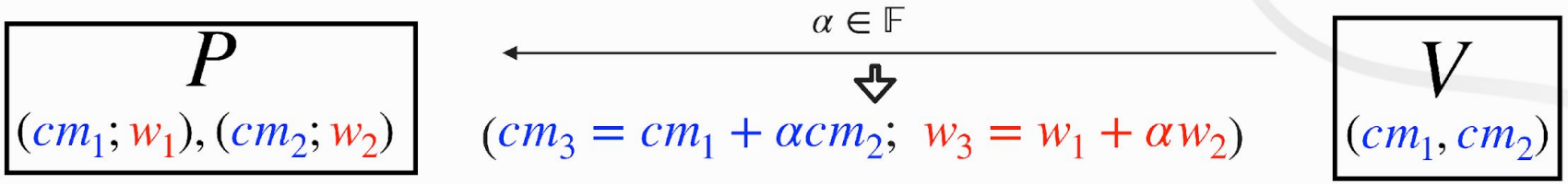


Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

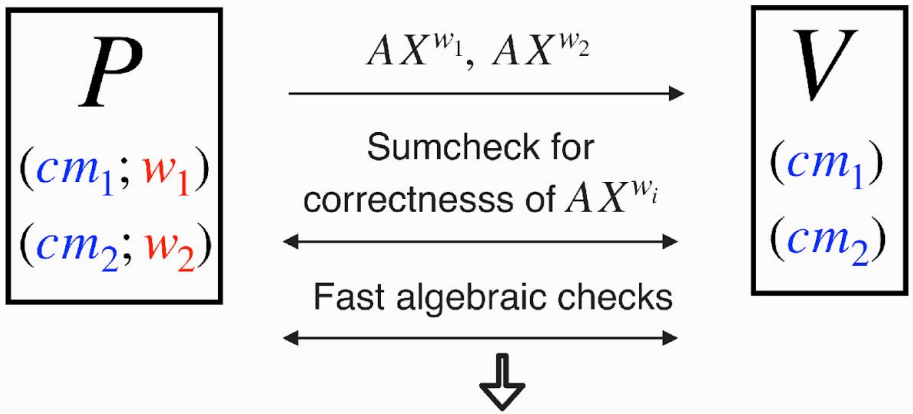


AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds



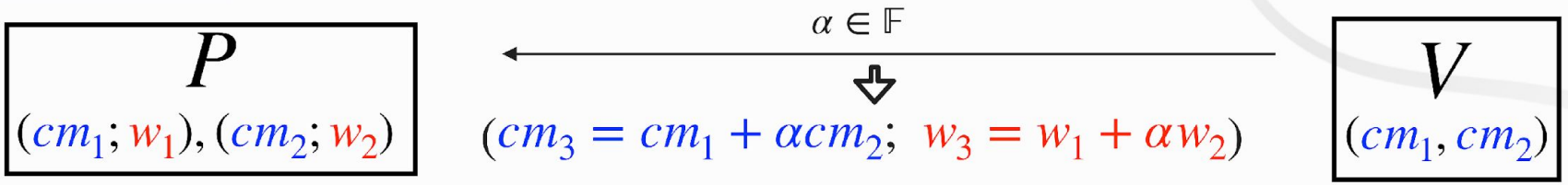
Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



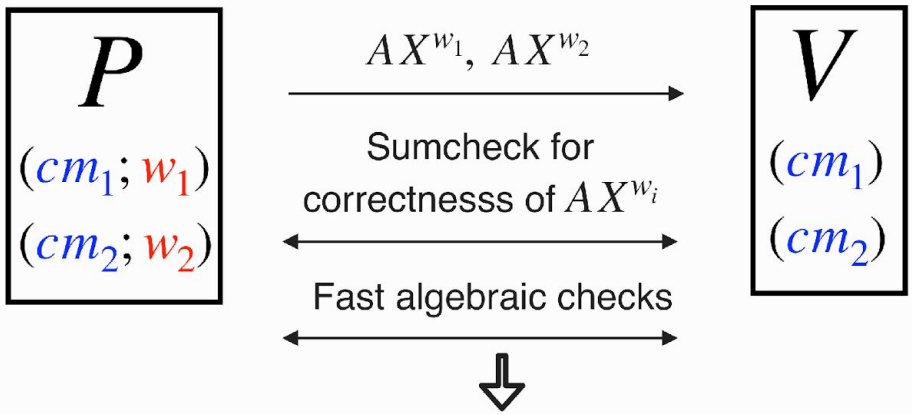
Claims about commitments, norm bounds and evaluations of multilinear polynomials

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$

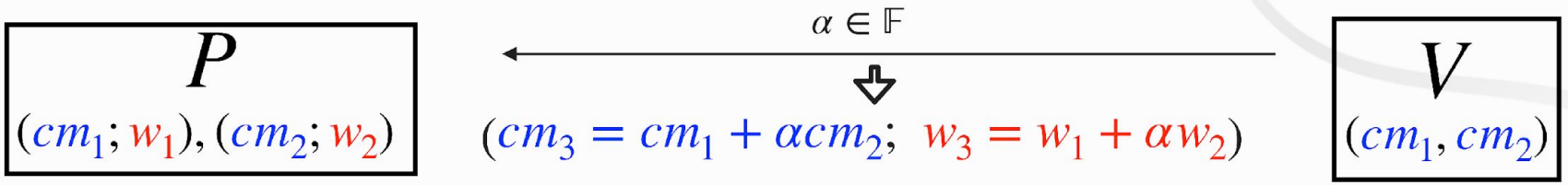


Claims about commitments, norm bounds and evaluations of multilinear polynomials

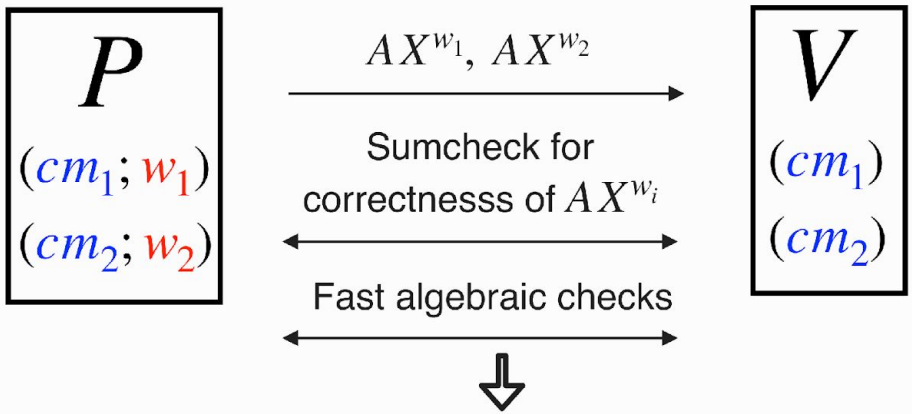
Estimated runtime

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



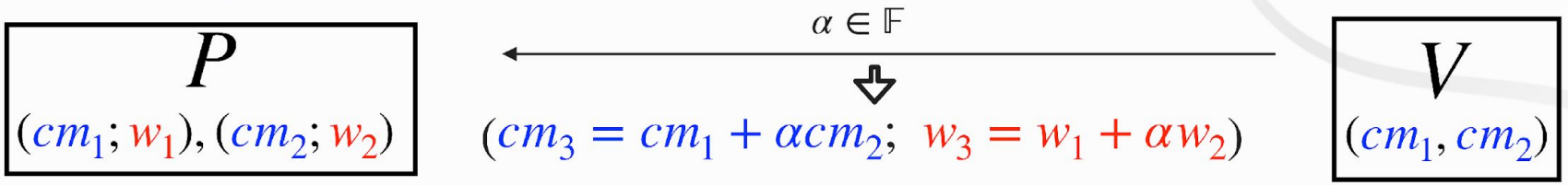
Claims about commitments, norm bounds and evaluations of multilinear polynomials

Estimated runtime

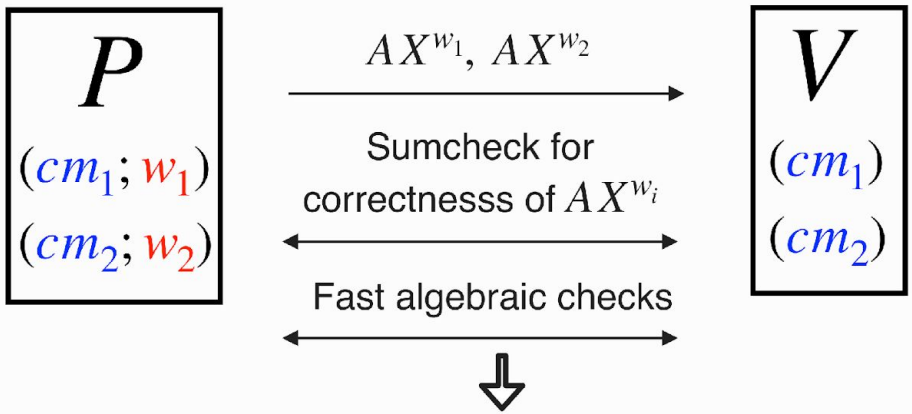
Dominating cost: $\deg(f) = 24$ degree 3 sumchecks over $\mathbb{F}_q$

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Solving norm bounds



Problem 2 Need to ask that $\|w\| \leq B$. $R_B = \{(cm; w) \mid Com(w) = cm,\ \|w\| \leq B\}$



Claims about commitments, norm bounds and evaluations of multilinear polynomials

Estimated runtime

Dominating cost: $\deg(f) = 24$ degree 3 sumchecks over $\mathbb{F}_q$

Estimate (extrapolation): 0.6-1s

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

The previous techniques
be used to fold CCS
constraints.

One decom
witness
B

Thanks

bits), $q \approx 2^{64}$.

$-X^{12}+1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

and $B = 2^8$.

old

CS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|	Linearize	LF+ decomp	LF norm bound	Total
2^13	2^16	170ms	~400ms	~600ms	~1.17s

or protocols

nova (from Sonobe implementation)

CCS witness	Total
2^16	1.2s

Neo (Nguyen, Setty, 2025)

WIP! (Very promising as well)

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM

Overall costs

The previous techniques
be used to fold CCS
constraints.

One decom
witness
B

Thanks

bits), $q \approx 2^{64}$.

$-X^{12}+1) \cong \mathbb{F}_{q^3} \times \overset{8}{\ldots} \times \mathbb{F}_{q^3}$

and $B = 2^8$.

old

CS witness	|w_1|, |w_2|	Linearize	LF decomp	LF norm bound	Total
2^13	2^16	170ms	3s	3s	6.17s

Latticefold+ (extrapolated, speculative)

CCS witness	|w_1|, |w_2|	Linearize	LF+ decomp	LF norm bound	Total
2^13	2^16	170ms	~400ms	~600ms	~1.17s

or protocols

nova (from Sonobe implementation)

CCS witness	Total
2^16	1.2s

Neo (Nguyen, Setty, 2025)

WIP! (Very promising as well)

NETHERMIND RESEARCH

AMD EPYC 7713 64-Core (with 6 cores available), 16GB of RAM