Spatial Isolation $\Rightarrow$ Zero Knowledge
Even in a Quantum World

Joint work with Alessandro Chiesa, Michael Forbes, and Nicholas Spooner
The problem
Zero Knowledge
Zero Knowledge
Zero Knowledge
Zero Knowledge
Zero Knowledge

Zero-Knowledge Proofs

[Goldwasser-Micali-Rackoff 89]
Zero Knowledge

Zero-Knowledge Proofs

Cryptographic assumptions (OWF)

ZK for NP

[Goldwasser-Micali-Rackoff 89]

[Goldreich-Micali-Wigderson 91]
Zero Knowledge

Zero-Knowledge Proofs

Cryptographic assumptions (OWF)
ZK for NP
[Goldreich-Micali-Wigderson 91]

Cryptographic assumptions are necessary
[Ostrovsky-Wigderson 93]

[Goldwasser-Micali-Rackoff 89]
Spatial Isolation $\Rightarrow$ Zero Knowledge

**Multi-prover Interactive Proofs (MIP)**

[BenOr-Goldwasser-Kilian-Wigderson 88]
Spatial Isolation ⇒ Zero Knowledge

Multi-prover Interactive Proofs (MIP)  [BenOr-Goldwasser-Kilian-Wigderson 88]
Spatial Isolation $\Rightarrow$ Zero Knowledge

Multi-prover Interactive Proofs (MIP) [BenOr-Goldwasser-Kilian-Wigderson 88]
Spatial Isolation $\Rightarrow$ Zero Knowledge

Multi-prover Interactive Proofs (MIP)

[BenOr-Goldwasser-Kilian-Wigderson 88]
Spatial Isolation $\Rightarrow$ Zero Knowledge

Multi-prover Interactive Proofs (MIP)

[BenOr-Goldwasser-Kilian-Wigderson 88]
Spatial Isolation $\Rightarrow$ Zero Knowledge

**Multi-prover Interactive Proofs (MIP)**

[BenOr-Goldwasser-Kilian-Wigderson 88]

Spatial isolation

Uncorrelated strategies

Unconditional ZK for NEXP

Spatial isolation

Uncorrelated strategies in a quantum world
Quantum Entanglement

MIP*  [Cleve-Hoyer-Toner-Watrous 04]
Quantum Entanglement

MIP* upper bounds?

[Cleve-Hoyer-Toner-Watrous 04]
Quantum Entanglement

MIP*

[Cleve-Hoyer-Toner-Watrous 04]

NEXP \subseteq MIP^*
[Itô-Vidick 12]
Quantum Entanglement

**MIP**

[Cleve-Hoyer-Toner-Watrous 04]

Does spatial isolation $\implies$ zero knowledge even in a quantum world?

**MIP**

upper bounds?

**NEXP $\subseteq$ MIP**

[Ito-Vidick 12]
Spatial isolation $\Rightarrow$ zero knowledge even in a quantum world

Yes!
Spatial isolation => zero knowledge
even in a quantum world

Theorem: \( \text{NEXP} \subseteq \text{ZK-MIP}^* \)
Spatial isolation \implies zero knowledge even in a quantum world

Theorem: \( \text{NEXP} \subseteq \text{ZK-MIP}^* \)

The challenge
Spatial isolation $\implies$ zero knowledge even in a quantum world

**Theorem:** $\text{NEXP} \subseteq \text{ZK-MIP}^*$

**The challenge**

We know that: $\text{NEXP} \subseteq \text{MIP}^*$ [IV12]
Spatial isolation => zero knowledge even in a quantum world

Theorem: $\text{NEXP} \subseteq \text{ZK-MIP}^*$

The challenge

We know that:

$\text{NEXP} \subseteq \text{MIP}^*$ [IV12]

$\text{NEXP} \subseteq \text{ZK-MIP}$ [BGKW88]
Spatial isolation => zero knowledge even in a quantum world

Theorem: $\text{NEXP} \subseteq \text{ZK-MIP}^*$

The challenge

We know that:

- $\text{NEXP} \subseteq \text{MIP}^*$ [IV12]
- $\text{NEXP} \subseteq \text{ZK-MIP}$ [BGKW88]
Spatial isolation => zero knowledge even in a quantum world

Theorem: \( \text{NEXP} \subseteq \text{ZK-MIP}^* \)

The challenge

We know that: \( \text{NEXP} \subseteq \text{MIP}^* \)  \[\text{[IV12]}\]
\( \text{NEXP} \subseteq \text{ZK-MIP} \)  \[\text{[BGKW88]}\]

Current MIP techniques are \textbf{ALGEBRAIC}

Why not combine them?
Spatial isolation $\Rightarrow$ zero knowledge even in a quantum world

**Theorem:** $\text{NEXP} \subseteq \text{ZK-MIP}^*$

**The challenge**

We know that:  
$\text{NEXP} \subseteq \text{MIP}^*$ \quad [\text{IV12}]  
$\text{NEXP} \subseteq \text{ZK-MIP}$ \quad [\text{BGKW88}]

Current MIP techniques are **ALGEBRAIC**

(Previous) zero-knowledge techniques were **COMBINATORIAL**
Spatial isolation => zero knowledge even in a quantum world

Theorem: $\text{NEXP} \subseteq \text{ZK-MIP}^*$

The challenge

We know that: $\text{NEXP} \subseteq \text{MIP}^*$ [IV12]

$\text{NEXP} \subseteq \text{ZK-MIP}$ [BGKW88]

Current MIP techniques are **ALGEBRAIC**

(Previous) zero-knowledge techniques were **COMBINATORIAL**

Technique Incompatibility

Why not combine them?
Spatial isolation $\Rightarrow$ zero knowledge

even in a quantum world
Spatial isolation $\Rightarrow$ zero knowledge even in a quantum world

**Theorem:** $\text{NEXP} \subseteq \text{ZK-MIP}^*$
Spatial isolation => zero knowledge even in a quantum world

Theorem: \( \text{NEXP} \subseteq \text{ZK-MIP}^* \)

Proof in 2 steps:

Lifting lemma

ZK-preserving
Spatial isolation => zero knowledge even in a quantum world

Theorem: $\text{NEXP} \subseteq \text{ZK-MIP}^*$

Proof in 2 steps:

Lifting lemma

Algebraic ZK
Interactive PCP

\[ \Downarrow \]

MIP*
Lifting Lemma: Any PCP $\rightarrow$ MIP* with similar parameters
Lifting Lemma: Any PCP $\xrightarrow{\text{MIP}^*}$ with similar parameters
Lifting Lemma: Any PCP $\xrightarrow{\text{MIP}^*}$ with similar parameters
From Classical to Quantum

**Lifting Lemma:** Any PCP $\rightarrow$ MIP* with similar parameters

All machines are CLASSICAL
From Classical to Quantum

Lifting Lemma: Any PCP $\Rightarrow$ MIP* with similar parameters

Abstraction of IV12’s $NEXP \subseteq MIP^*$

All machines are CLASSICAL
Lifting Lemma: Any interactive PCP $\xrightarrow{\text{MIP}^* \text{ with similar parameters}}$
Lifting Lemma: Any “low-degree” interactive PCP $\rightarrow$ MIP* with similar parameters

PRESERVING ZK

Low-degree Interactive PCP

All machines are CLASSICAL

[Kalai-Raz 08]
From Classical to Quantum

Lifting Lemma: Any "low-degree" interactive PCP $\rightarrow$ MIP* with similar parameters

PRESERVING ZK

Low-degree Interactive PCP

[Kalai-Raz 08]

All machines are CLASSICAL
Overview of the Lifting Lemma
Overview of the Lifting Lemma

w.p. 1/2: MIP* point-vs-plane
    Low-degree test
    [Natarajan-Vidick 18]
Overview of the Lifting Lemma

w.p. 1/2:  MIP* point-vs-plane
Low-degree test
[Natarajan-Vidick 18]
Overview of the Lifting Lemma

w.p. 1/2: MIP* point-vs-plane
Low-degree test
[Natarajan-Vidick 18]
Overview of the Lifting Lemma

w.p. 1/2:  MIP* point-vs-plane
Low-degree test
[Natarajan-Vidick 18]
Overview of the Lifting Lemma

w.p. 1/2:  MIP* point-vs-plane
Low-degree test
[Natarajan-Vidick 18]
Overview of the Lifting Lemma

w.p. 1/2: MIP* point-vs-plane
Low-degree test
[Natarajan-Vidick 18]
Overview of the Lifting Lemma

w.p. 1/2: **MIP* point-vs-plane**

**Low-degree test**

[Natarajan-Vidick 18]
Overview of the Lifting Lemma

w.p. 1/2: Interactive PCP emulation

MIP*
Overview of the Lifting Lemma

w.p. 1/2: Interactive PCP emulation
Overview of the Lifting Lemma

w.p. 1/2: Interactive PCP emulation

MIP*
Algebraic Zero Knowledge
**Theorem:** There exists a ZERO KNOWLEDGE low-degree interactive PCP for NEXP
Theorem: There exists a ZERO KNOWLEDGE low-degree interactive PCP for NEXP

Previous ZK techniques are Incompatible with algebraic lifting
Algebraic Zero Knowledge

**Theorem:** There exists a ZERO KNOWLEDGE low-degree interactive PCP for NEXP

- **Strong ZK sumcheck**
- **Algebraic Commitment scheme**
- **Structural results on Reed-Muller subcube sums**
- **Weak ZK sumcheck** [BCFGRS17]
- **Succinct constraint detection for Reed-Muller** [BCFGRS17]
- **Derandomized PIT for sums of products of Reed-Solomon** [RS05]
Algebraic Zero Knowledge

Theorem: There exists a ZERO KNOWLEDGE low-degree interactive PCP for NEXP

- Strong ZK sumcheck
- Weak ZK sumcheck [BCFGRS17]
- Structural results on Reed-Muller subcube sums
- Succinct constraint detection for Reed-Muller [BCFGRS17]
- Derandomized PIT for sums of products of Reed-Solomon [RS05]

Previous ZK techniques are Incompatible with algebraic lifting
First some high-level motivation
First some high-level motivation
First some high-level motivation

**Goal:** commit to a message $\beta \in \mathbb{F}$

perfectly **HIDING** the message

in a statistically **BINDING** way
Algebraic Commitment Scheme

First some high-level motivation

Goal: commit to a message $\beta \in \mathbb{F}$ perfectly HIDING the message in a statistically BINDING way

How: send a random polynomial $p \in \text{RM}_q[m,r]$ such that

$$\sum_{\alpha \in H^m} p(\alpha) = \beta$$
Algebraic Commitment Scheme

First some high-level motivation

**Goal:** commit to a message \( \beta \in \mathbb{F} \)
perfectly HIDING the message
in a statistically BINDING way

**How:** send a random polynomial
\( p \) s.t.
\[ \sum_{\alpha \in H^m} p(\alpha) = \beta \]
de-commit via interaction
Warmup: Subcube Sums of Reed-Muller

\[ \text{RM}_q[m,r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r}[X_1, \ldots, X_m] \} \]
Warmup: Subcube Sums of Reed-Muller

\[ \text{RM}_q [m, r] = \{ \langle p(\alpha) \rangle \mid p \in F_q^{\leq r} [X_1, \ldots, X_m] \} \]

Low-degree extension perspective

\[ H \subseteq F \quad |H| < r \]
Warmup: Subcube Sums of Reed-Muller

\[
\text{RM}_q[m,r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_{q}^{\leq r}[X_1,\ldots,X_m]\}
\]

Low-degree extension perspective

\[
H \subseteq \mathbb{F} \quad |H| < r
\]
Warmup: Subcube Sums of Reed-Muller

$$\text{RM}_q[m,r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r}[X_1,\ldots,X_m] \}$$

**Low-degree extension perspective**

$$H \subseteq \mathbb{F} \quad |H| < r$$

For $$f : H^m \rightarrow \mathbb{F}$$

$$\sum_{\alpha \in H^m} f(\alpha)$$ is \#P-hard to compute
Warmup: Subcube Sums of Reed-Muller

\[ \mathbf{RM}_q[m, r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r}[X_1, \ldots, X_m] \} \]

**Low-degree extension perspective**

\[ H \subseteq \mathbb{F} \quad |H| < r \]

**The problem: a simple case**

For \( f : H^m \rightarrow \mathbb{F} \)

\[ \sum_{\alpha \in H^m} f(\alpha) \text{ is \#P-hard to compute} \]

Given

\[ \begin{bmatrix} p \in \mathbf{RM}_q[m, r] \\ p(\alpha) = f(\alpha) \quad \forall \alpha \in H^m \end{bmatrix} \]
Warmup: Subcube Sums of Reed-Muller

$$RM_q[m,r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r} [X_1, \ldots, X_m] \}$$

Low-degree extension perspective

\[ H \subseteq \mathbb{F} \quad |H| < r \]

For \( f : H^m \rightarrow \mathbb{F} \)

\( \sum_{\alpha \in H^m} f(\alpha) \) is \#P-hard to compute

The problem: a simple case

Given \( p \in RM_q[m,r] \)

\[ p(\alpha) = f(\alpha) \quad \forall \alpha \in H^m \]

Is \( \sum_{\alpha \in H^m} p(\alpha) \) still hard to compute?
Warmup: Subcube Sums of Reed-Muller

\[ \text{RM}_q[m, r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r}[X_1, \ldots, X_m] \} \]

**Low-degree extension perspective**

\[ H \subseteq \mathbb{F} \quad |H| < r \]

**For** \( f : H^m \rightarrow \mathbb{F} \)

\[ \sum_{\alpha \in H^m} f(\alpha) \] is \( \#P \)-hard to compute

**The problem: a simple case**

Given \( p \in \text{RM}_q[m, r] \)

\[ p(\alpha) = f(\alpha) \quad \forall \alpha \in H^m \]

Is \( \sum_{\alpha \in H^m} p(\alpha) \) still hard to compute?

**Algebrization framework**

[Aaronson-Wigderson 09]
Warmup: Subcube Sums of Reed-Muller

\[ \text{RM}_q[m,r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r}[X_1,\ldots,X_m] \} \]

**Low-degree extension perspective**

\[ H \subseteq \mathbb{F} \quad |H| < r \]

For \( f : H^m \rightarrow \mathbb{F} \)

\[ \sum_{\alpha \in H^m} f(\alpha) \text{ is \#P-hard to compute} \]

**The problem: a simple case**

Given \( p \in \text{RM}_q[m,r] \)

\[ p(\alpha) = f(\alpha) \quad \forall \alpha \in H^m \]

Is \( \sum_{\alpha \in H^m} p(\alpha) \) still hard to compute?

For \( r=1, H=\{0,1\} \)

(multilinear extension)

\[ p(2^{-1},\ldots,2^{-1}) = 2^{-k} \sum_{\alpha \in H^m} p(\alpha) \]

**NO!**

[JKRS09]
Warmup: Subcube Sums of Reed-Muller

Warmup: Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \) then computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries.
Warmup: Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \), computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries.

Suppose \( H = \{0,1\} \)

\[ p \in \text{RM}_q[m,r] \]

\[ H^m \]
Warmup: Subcube Sums of Reed-Muller

Warmup: Let $p \in \text{RM}_q[m,r]$

If $r \geq 2$, computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries.

Suppose $H=\{0,1\}$

Approach: Reduction from communication complexity
Warmup: Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \), computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries.

Suppose \( H = \{0,1\} \)

Approach: Reduction from communication complexity

\( x \in \{0,1\}^n \)
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let $p \in \text{RM}_q[m,r]

If $r \geq 2$ \hspace{1cm} \text{Computing } \sum_{\alpha \in H^m} p(\alpha) \hspace{1cm} \text{takes } \tilde{\Omega}(|H^m|) \text{ queries}

Suppose $H=\{0,1\}$

**Approach:** Reduction from communication complexity

$x \in \{0,1\}^n \hspace{1cm} y \in \{0,1\}^n$
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let $p \in \text{RM}_q[m,r]$

If $r \geq 2$ then computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries.

Suppose $H=\{0,1\}$

**Approach:** Reduction from communication complexity

$x \in \{0,1\}^n$  \hspace{1cm}  $y \in \{0,1\}^n$
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \) → Computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries

Suppose \( H=\{0,1\} \)

**Approach:** Reduction from communication complexity

\[ x \in \{0,1\}^n \quad \quad y \in \{0,1\}^n \]

\( \Omega(n) \) communication required to decide unique-disjointness: \( \exists! \quad x_i = y_i = 1 \)
Warmup: Let $p \in \text{RM}_{q}[m,r]$

If $r \geq 2$ Computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries.

Suppose $H=\{0,1\}$

Approach: Reduction from communication complexity

$\Omega(n)$ communication required to decide unique-disjointness: $\exists! \quad x_i = y_i = 1$

Towards contradiction: suppose $\sum_{\alpha \in H^m} p(\alpha)$ computable with $\tilde{o}(|H^m|)$ queries
Warmup: Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \), computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries.

Suppose \( H = \{0,1\} \)

Approach: Reduction from communication complexity

\( x \in \{0,1\}^n \quad y \in \{0,1\}^n \)

\( \Omega(n) \) communication required to decide unique-disjointness: \( \exists! \quad x_i = y_i = 1 \)

Towards contradiction: suppose \( \sum_{\alpha \in H^m} p(\alpha) \) computable with \( \tilde{o}(|H^m|) \) queries

Construct a protocol for unique disjointness!
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \), computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}( |H^m| ) \) queries.

**The protocol**

Towards contradiction:

\[ \sum_{\alpha \in H^m} p(\alpha) \text{ computable with } \tilde{\Theta}( |H^m| ) \text{ queries} \]

**Reduction from communication complexity**

For some \( x \in \{0,1\}^n \) and \( y \in \{0,1\}^n \), \( \Omega(n) \) communication required to decide if \( \exists i : x_i = y_i = 1 \).
Warmup: Subcube Sums of Reed-Muller

Warmup: Let $p \in \text{RM}_q[m,r]$

If $r \geq 2$ → Computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries

The protocol

$x \in \{0,1\}^n$

Towards contradiction:

$\sum_{\alpha \in H^m} p(\alpha)$ computable with $\tilde{o}(|H^m|)$ queries

Reduction from communication complexity

$x \in \{0,1\}^n$  $y \in \{0,1\}^n$

$\Omega(n)$ communication required to decide if $\exists! \quad x_i = y_i = 1$
Warmup: Subcube Sums of Reed-Muller

Warmup: Let \( p \in \operatorname{RM}_q [m,r] \)

If \( r \geq 2 \) \( \Rightarrow \) Computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries

The protocol

\[ x \in \{0,1\}^n \]
\[ f_x : H^m \rightarrow \{0,1\} \]

Towards contradiction:

\[ \sum_{\alpha \in H^m} p(\alpha) \text{ computable with } \tilde{\Theta}(|H^m|) \text{ queries} \]

Reduction from communication complexity:

\[ x \in \{0,1\}^n \]
\[ y \in \{0,1\}^n \]
\[ \Omega(n) \text{ communication required to decide if } \exists! \ x_i = y_i = 1 \]
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let $p \in \text{RM}_q[m,r]$

If $r \geq 2$ \quad Computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries

The protocol

$x \in \{0,1\}^n$

$f_x : H^m \rightarrow \{0,1\}$

$p_x : \mathbb{F}^m \rightarrow \mathbb{F}$

Towards contradiction:

$\sum_{\alpha \in H^m} p(\alpha)$ computable with $\tilde{\Theta}(|H^m|)$ queries

Reduction from communication complexity

$x \in \{0,1\}^n$ \quad $y \in \{0,1\}^n$

$\Omega(n)$ communication required to decide if $\exists! \; x_i = y_i = 1$
Warmup: Let $p \in \text{RM}_q[m,r]$.

If $r \geq 2$, computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries.

The protocol:

$x \in \{0,1\}^n$
$f_x : H^m \to \{0,1\}$
$p_x : \mathbb{F}^m \to \mathbb{F}$

$y \in \{0,1\}^n$
$f_y : H^m \to \{0,1\}$
$p_y : \mathbb{F}^m \to \mathbb{F}$

Towards contradiction:

$\sum_{\alpha \in H^m} p(\alpha)$ computable with $\tilde{\Omega}(|H^m|)$ queries.

Reduction from communication complexity:

$x \in \{0,1\}^n$
$y \in \{0,1\}^n$

$\Omega(n)$ communication required to decide if $\exists! i \ x_i = y_i = 1$.
Warmup: Subcube Sums of Reed-Muller

Warmup: Let \( p \in \mathbb{R}M_q [m, r] \)

If \( r \geq 2 \) \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries

The protocol

\[ x \in \{0,1\}^n \]
\[ f_x : H^m \rightarrow \{0,1\} \]
\[ p_x : \mathbb{F}^m \rightarrow \mathbb{F} \]

\[ y \in \{0,1\}^n \]
\[ f_y : H^m \rightarrow \{0,1\} \]
\[ p_y : \mathbb{F}^m \rightarrow \mathbb{F} \]

\[ p(\alpha) = p_x(\alpha) \cdot p_y(\alpha) \]

Towards contradiction:

\[ \sum_{\alpha \in H^m} p(\alpha) \] computable with \( \tilde{\Theta}(|H^m|) \) queries

Reduction from communication complexity

\[ x \in \{0,1\}^n \]
\[ y \in \{0,1\}^n \]
\[ \Omega(n) \] communication required to decide if \( \exists! \ x_i = y_i = 1 \)
Warmup: Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \) Computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(\lvert H^m \rvert) \) queries

\[ x \in \{0,1\}^n \]
\[ f_x : H^m \to \{0,1\} \]
\[ p_x : \mathbb{F}^m \to \mathbb{F} \]

\[ y \in \{0,1\}^n \]
\[ f_y : H^m \to \{0,1\} \]
\[ p_y : \mathbb{F}^m \to \mathbb{F} \]

\[ p(\alpha) = p_x(\alpha) \cdot p_y(\alpha) \]

Towards contradiction:

\[ \sum_{\alpha \in H^m} p(\alpha) \text{ computable with } \tilde{o}(\lvert H^m \rvert) \text{ queries} \]
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let \( p \in \mathsf{RM}_q[m,r] \)

If \( r \geq 2 \) then Computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries.

**The protocol**

\[
\begin{align*}
    & x \in \{0,1\}^n \\
    & f_x : H^m \rightarrow \{0,1\} \\
    & p_x : F^m \rightarrow F \\
    & y \in \{0,1\}^n \\
    & f_y : H^m \rightarrow \{0,1\} \\
    & p_y : F^m \rightarrow F
\end{align*}
\]

\[
p(\alpha) = p_x(\alpha) \cdot p_y(\alpha)
\]

\((x, y) \in \text{DISJ}\)

Towards contradiction:

\[
\sum_{\alpha \in H^m} p(\alpha) \text{ computable with } \tilde{\Omega}(|H^m|) \text{ queries}
\]
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let $p \in \text{RM}_q[m,r]$.

If $r \geq 2$ then Computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries.

**The protocol**

$x \in \{0,1\}^n$
$f_x : H^m \rightarrow \{0,1\}$
$p_x : F^m \rightarrow F$

$y \in \{0,1\}^n$
$f_y : H^m \rightarrow \{0,1\}$
$p_y : F^m \rightarrow F$

$(x, y) \in \text{DISJ} \iff \sum_{\alpha \in H^m} f_x(\alpha) \cdot f_y(\alpha) = 0$

Towards contradiction:

$\sum_{\alpha \in H^m} p(\alpha)$ computable with $\tilde{\Omega}(|H^m|)$ queries.

Reduction from communication complexity

$x \in \{0,1\}^n$
$y \in \{0,1\}^n$

$\exists i \ s.t. x_i = y_i = 1$
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let \( p \in \text{RM}_q [m, r] \)

If \( r \geq 2 \), computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries.

**The protocol**

\[
x \in \{0,1\}^n \\
f_x : H^m \rightarrow \{0,1\} \\
p_x : F^m \rightarrow F
\]

\[
y \in \{0,1\}^n \\
f_y : H^m \rightarrow \{0,1\} \\
p_y : F^m \rightarrow F
\]

\[
p(\alpha) = p_x(\alpha) \cdot p_y(\alpha)
\]

\[
(x, y) \in \text{DISJ} \quad \sum_{\alpha \in H^m} f_x(\alpha) \cdot f_y(\alpha) = 0 \quad \sum_{\alpha \in H^m} p(\alpha) = 0
\]

Towards contradiction:

\[
\sum_{\alpha \in H^m} p(\alpha) \text{ computable with } \tilde{\Theta}(|H^m|) \text{ queries}
\]
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \) \( \implies \) Computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries

\[ x \in \{0,1\}^n \]
\[ f_x : H^m \to \{0,1\} \]
\[ p_x : \mathbb{F}^m \to \mathbb{F} \]

\[ y \in \{0,1\}^n \]
\[ f_y : H^m \to \{0,1\} \]
\[ p_y : \mathbb{F}^m \to \mathbb{F} \]

\[ p(\alpha) = p_x(\alpha) \cdot p_y(\alpha) \]

\( (x,y) \in \text{DISJ} \) \( \implies \) \( \sum_{\alpha \in H^m} f_x(\alpha) \cdot f_y(\alpha) = 0 \) \( \implies \) \( \sum_{\alpha \in H^m} p(\alpha) = 0 \)

\( (x,y) \notin \text{DISJ} \)

Towards contradiction:
\[ \sum_{\alpha \in H^m} p(\alpha) \text{ computable with } \tilde{\Omega}(|H^m|) \text{ queries} \]

Reduction from communication complexity
\[ \Omega(n) \text{ communication required to decide if } \exists! \ x_i = y_i = 1 \]
Warmup: Subcube Sums of Reed-Muller

**Warmup:** Let \( p \in \text{RM}_q\{m,r\} \)

If \( r \geq 2 \) \( \implies \) Computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}( |H^m| ) \) queries

The protocol

\( x \in \{0,1\}^n \)
\( f_x : H^m \to \{0,1\} \)
\( p_x : \mathbb{F}^m \to \mathbb{F} \)

\( y \in \{0,1\}^n \)
\( f_y : H^m \to \{0,1\} \)
\( p_y : \mathbb{F}^m \to \mathbb{F} \)

\( p(\alpha) = p_x(\alpha) \cdot p_y(\alpha) \)

\((x, y) \in \text{DISJ} \implies \sum_{\alpha \in H^m} f_x(\alpha) \cdot f_y(\alpha) = 0 \implies \sum_{\alpha \in H^m} p(\alpha) = 0\)

\((x, y) \notin \text{DISJ} \implies \sum_{\alpha \in H^m} f_x(\alpha) \cdot f_y(\alpha) = 1\)

Towards contradiction:

\( \sum_{\alpha \in H^m} p(\alpha) \) computable with \( \tilde{o}( |H^m| ) \) queries

Reduction from communication complexity

\( x \in \{0,1\}^n \)
\( \exists! \ x_i = y_i = 1 \)

\( \Omega(n) \) communication required to decide if
Warmup: Subcube Sums of Reed-Muller

Warmup: Let $p \in \text{RM}_q[m,r]$

If $r \geq 2$ Computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries

The protocol

$x \in \{0,1\}^n$
$f_x : H^m \to \{0,1\}$
$p_x : \mathbb{F}^m \to \mathbb{F}$

$y \in \{0,1\}^n$
$f_y : H^m \to \{0,1\}$
$p_y : \mathbb{F}^m \to \mathbb{F}$

$p(\alpha) = p_x(\alpha) \cdot p_y(\alpha)$

$(x, y) \in \text{DISJ}$ $\sum_{\alpha \in H^m} f_x(\alpha) \cdot f_y(\alpha) = 0$ $\sum_{\alpha \in H^m} p(\alpha) = 0$

$(x, y) \not\in \text{DISJ}$ $\sum_{\alpha \in H^m} f_x(\alpha) \cdot f_y(\alpha) = 1$ $\sum_{\alpha \in H^m} p(\alpha) = 1$

Towards contradiction:

$\sum_{\alpha \in H^m} p(\alpha)$ computable with $\tilde{o}(|H^m|)$ queries

Reduction from communication complexity

$x \in \{0,1\}^n$ $y \in \{0,1\}^n$

$\Omega(n)$ communication required to decide if $\exists! x_i = y_i = 1$
**Warmup:** Let $p \in RM_q[m,r]$

If $r \geq 2$ then computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries

---

The protocol

$x \in \{0,1\}^n$

$f_x : H^m \rightarrow \{0,1\}$

$p_x : \mathbb{F}^m \rightarrow \mathbb{F}$

$y \in \{0,1\}^n$

$f_y : H^m \rightarrow \{0,1\}$

$p_y : \mathbb{F}^m \rightarrow \mathbb{F}$

$$p(\alpha) = p_x(\alpha) \cdot p_y(\alpha)$$

$(x,y) \in \text{DISJ} \quad \sum_{\alpha \in H^m} f_x(\alpha) \cdot f_y(\alpha) = 0 \quad \sum_{\alpha \in H^m} p(\alpha) = 0$

$(x,y) \not\in \text{DISJ} \quad \sum_{\alpha \in H^m} f_x(\alpha) \cdot f_y(\alpha) = 1 \quad \sum_{\alpha \in H^m} p(\alpha) = 1$

---

Towards contradiction:

$\sum_{\alpha \in H^m} p(\alpha)$ computable with $\tilde{\Theta}(|H^m|)$ queries

Reduction from communication complexity

$x \in \{0,1\}^n$

$y \in \{0,1\}^n$

$\Omega(n)$ communication required to decide if $\exists! \quad x_i = y_i = 1$
Warmup: Let $p \in \text{RM}_q[m,r]$

If $r \geq 2$, computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries

So far, we showed:
What is missing?

So far, we showed:

**Warmup:** Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \) \( \sum_{\alpha \in H^m} p(\alpha) \) Computing takes \( \tilde{\Omega}(|H^m|) \) queries

This suffices for committing to an ELEMENT
What is missing?

So far, we showed:

**Warmup:** Let \( p \in \text{RM}_q[m,r] \)

If \( r \geq 2 \) Computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \Omega(|H^m|) \) queries

This suffices for committing to an ELEMENT

We need to commit to a POLYNOMIAL!
What is missing?

So far, we showed:

**Warmup:** Let $p \in \text{RM}_q[m,r]$

If $r \geq 2$ Computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}(|H^m|)$ queries

This suffices for committing to an ELEMENT

We need to commit to a POLYNOMIAL!

Now, we wish to de-commit w.r.t. a single point
What is missing?

So far, we showed:

**Warmup**: Let \( p \in \mathbb{R}M_q [m, r] \)

If \( r \geq 2 \), computing \( \sum_{\alpha \in H^m} p(\alpha) \) takes \( \tilde{\Omega}(|H^m|) \) queries.

This suffices for committing to an ELEMENT.

We need to commit to a POLYNOMIAL!

Now, we wish to de-commit w.r.t. a single point

WITHOUT LEAKING information about other points.
So far, we showed:

**Warmup:** Let $p \in \text{RM}_q[m,r]$

If $r \geq 2$ Computing $\sum_{\alpha \in H^m} p(\alpha)$ takes $\tilde{\Omega}( |H^m| )$ queries

This suffices for committing to an ELEMENT

**We need to commit to a POLYNOMIAL!**

Now, we wish to de-commit w.r.t. a single point

WITHOUT LEAKING information about other points

Requires new algebraic complexity lower bounds!
The General Case: Reed-Muller Subcube Sums

$$\text{RM}_q[m,r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r}[X_1,\ldots,X_m] \}$$
The General Case: Reed-Muller Subcube Sums

\[ \text{RM}_q[m,r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r}[X_1,\ldots,X_m] \} \]

Given \( p \), not only the sum over the whole cube

\[ \sum_{\alpha_1,\ldots,\alpha_m \in H} p(\alpha_1,\ldots,\alpha_m) \]

is hard to compute.
The General Case: Reed-Muller Subcube Sums

\[ \text{RM}_q [m,r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r} [X_1, \ldots, X_m] \} \]

Given \( p \), not only the sum over the whole cube
\[ \sum_{\alpha_1, \ldots, \alpha_m \in H} p(\alpha_1, \ldots, \alpha_m) \] is hard to compute

But also partial (subcube) sums!
The General Case: Reed-Muller Subcube Sums

Given $p$, not only the sum over the whole cube
\[
\sum_{\alpha_1, \ldots, \alpha_m \in H} p(\alpha_1, \ldots, \alpha_m)
\]
is hard to compute

But also partial (subcube) sums!
\[
\langle \sum_{z_1} p(z_1, \alpha_2, \ldots, \alpha_m) \rangle_{z_1 \in \mathbb{F}}
\]
The General Case: Reed-Muller Subcube Sums

\[ \text{RM}_q[m,r] = \{ \langle p(\alpha) \rangle \mid p \in F_q^{\leq r}[X_1,\ldots,X_m] \} \]

Given \( p \), not only the sum over the whole cube

\[ \sum_{\alpha_1,\ldots,\alpha_m \in H} p(\alpha_1,\ldots,\alpha_m) \]

is hard to compute

But also partial (subcube) sums!

\[ \langle \sum p(z_1,\alpha_2,\ldots,\alpha_m) \rangle_{z_1 \in F} \]
\[ \langle \sum p(z_1,z_2,\alpha_3,\ldots,\alpha_m) \rangle_{z_1,z_2 \in F} \]
\[ \langle \sum p(z_1,\ldots,z_{m-1},\alpha_m) \rangle_{z_1,\ldots,z_{m-1} \in F} \]
The General Case: Reed-Muller Subcube Sums

\[ \text{RM}_q [m,r] = \{ \langle p(\alpha) \rangle \mid p \in \mathbb{F}_q^{\leq r}[X_1,\ldots,X_m] \} \]

Given \( p \), not only the sum over the whole cube
\[ \sum_{\alpha_1,\ldots,\alpha_m \in H} p(\alpha_1,\ldots,\alpha_m) \] is hard to compute

But also partial (subcube) sums!

\[ \langle \sum p(z_1,\alpha_2,\ldots,\alpha_m) \rangle_{z_1 \in \mathbb{F}} \]
\[ \langle \sum p(z_1,z_2,\alpha_3,\ldots,\alpha_m) \rangle_{z_1,z_2 \in \mathbb{F}} \]
\[ \langle \sum p(z_1,\ldots,z_{m-1},\alpha_m) \rangle_{z_1,\ldots,z_{m-1} \in \mathbb{F}} \]

and their linear combinations!
The General Case: Reed-Muller Subcube Sums

Extending the low-degree extension!

Given \( p \), not only the sum over the whole cube

\[
\sum_{\alpha_1, \ldots, \alpha_m \in H} p(\alpha_1, \ldots, \alpha_m)
\]

is hard to compute

But also partial (subcube) sums!

\[
\langle \sum p(z_1, \alpha_2, \ldots, \alpha_m) \rangle_{z_1 \in \mathbb{F}}
\]

\[
\langle \sum p(z_1, z_2, \alpha_3, \ldots, \alpha_m) \rangle_{z_1, z_2 \in \mathbb{F}}
\]

\[
\langle \sum p(z_1, \ldots, z_{m-1}, \alpha_m) \rangle_{z_1, \ldots, z_{m-1} \in \mathbb{F}}
\]
The General Case: Reed-Muller Subcube Sums

Extending the low-degree extension!

Given $p$, not only the sum over the whole cube
$$\sum_{\alpha_1, \ldots, \alpha_m \in H} p(\alpha_1, \ldots, \alpha_m)$$ is hard to compute

But also partial (subcube) sums!

$$\langle \sum p(z_1, \alpha_2, \ldots, \alpha_m) \rangle_{z_1 \in F}$$
$$\langle \sum p(z_1, z_2, \alpha_3, \ldots, \alpha_m) \rangle_{z_1, z_2 \in F}$$
$$\langle \sum p(z_1, \ldots, z_{m-1}, \alpha_m) \rangle_{z_1, \ldots, z_{m-1} \in F}$$

and their linear combinations!

Theorem: Let $p \in RM_q[m,r]$

If $r \geq 2$ $\forall \alpha \in H^\ell$ computing $\sum_{\alpha \in H^\ell} p(z, \alpha)$ takes $\tilde{\Omega}(|H^\ell|)$ queries
Open Questions
Open Questions

\[ \text{NEXP} \subseteq \text{ZK-MIP}^* \]

with O(1) rounds
Open Questions

NEXP \subseteq \text{ZK-MIP}^* \\
with O(1) rounds \\

Lifting a richer class of protocols
Open Questions

\( \text{NEXP} \subseteq \text{ZK-MIP}^* \)
with \( O(1) \) rounds

Lifting a richer class of protocols

Entanglement-resistant Tensor code testing
Thank you!