Fast RS-IOP Multivariate Polynomial Commitments and Verifiable Secret Sharing

Zongyang Zhang, Weihan Li, Yanpei Guo, and Kexin Shi, Beihang University; Sherman S. M. Chow, The Chinese University of Hong Kong; Ximeng Liu, Fuzhou University; Jin Dong, Beijing Academy of Blockchain and Edge Computing

https://www.usenix.org/conference/usenixsecurity24/presentation/zhang-zongyang

This paper is included in the Proceedings of the 33rd USENIX Security Symposium.
August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Open access to the Proceedings of the 33rd USENIX Security Symposium is sponsored by USENIX.
Fast RS-IOP Multivariate Polynomial Commitments and Verifiable Secret Sharing

Zongyang Zhang† Weihan Li†‡ Yanpei Guo* Kexin Shi*
Sherman S. M. Chow‡ Ximeng Liu§ Jin Dong¶

Abstract

Supporting proofs of evaluations, polynomial commitment schemes (PCS) are crucial in secure distributed systems. Schemes based on fast Reed–Solomon interactive oracle proofs (RS-IOP) of proximity have recently emerged, offering transparent setup, plausible post-quantum security, efficient operations, and, notably, sublinear proof size and verification. Manifesting a new paradigm, PCS with one-to-many proof can enhance the performance of (asynchronous) verifiable secret sharing ((A)VSS), a cornerstone in distributed computing, for proving multiple evaluations to multiple verifiers. Current RS-IOP-based multivariate PCS, including Hyper-Plonk (Eurocrypt ’23) and Virgo (S&P ’20), however, only offer quasi-linear prover complexity in the polynomial size.

We propose PolyFRIM, a fast RS-IOP-based multivariate PCS with optimal linear prover complexity, 5-25× faster than prior arts while ensuring competent proof size and verification. Hedging the challenging absence of FFT circuits for multivariate evaluation, PolyFRIM surpasses Zhang et al.’s (Usenix Sec. ’22) one-to-many univariate PCS, accelerating proving by 4-7× and verification by 2-4× with 25% shorter proof. Leveraging PolyFRIM, we propose an AVSS scheme FRISS with a better efficiency tradeoff than prior arts from multivariate PCS, including Bingo (Crypto ’23) and Haven (FC ’21).

1 Introduction

A polynomial commitment scheme (PCS) enables a prover to commit to a polynomial \( f \) defined over a field \( F \) with degree \( d \) and variable number \( \mu \). When given a point \( x \in \mathbb{F}^d \), the prover can convince a verifier via an evaluation proof that the committed polynomial \( f \) satisfies \( f(x) = y \) for a public \( y \in \mathbb{F} \). A PCS is succinct if the size of the proof/transcript is sublinear in the polynomial size \( d^\mu \) and is efficient if verification time is sublinear in \( d^\mu \). Succinct and efficient PCS is integral in recent zero-knowledge succinct non-interactive argument of knowledge (zk-SNARKs) [16,20,29] via integrating PCS with polynomial interactive oracle proofs (IOPs) [8].


Adapting the first PCS from FRI [32] (FRI-PC henceforth), tailored for univariate polynomials, to multivariate PCS poses challenges without additive homomorphism [26]. Hyper-Plonk [16, §B] (only work for \( d = 2 \)) and Virgo [37] represent the latest FRI-based multivariate PCSs. Their prover complexity is \( O(\mu \cdot d^\mu \log d) \), in contrast to \( O(d^\mu) \) FRI-PC (for \( \mu = 1 \)). In Virgo, the prover needs to invoke the Goldwasser–Kalai–Rothblum (GKR) protocol [21] for fast Fourier transformation (FFT) with a statement size of \( O(\mu \cdot d^\mu \log d) \), incurring a prover complexity quasi-linear to the polynomial size \( d^\mu \). Hyper-Plonk is simpler without needing the GKR composition.

A PCS with one-to-many proofs [31] allows a prover to open distinct evaluations of a single committed polynomial, where each evaluation corresponds to a unique verifier with a lower prover complexity than repeating single proof. Zhang et al. (ZXH ’22) [36] propose a framework for one-to-many proof of transparent univariate polynomials, including...
a polynomial interactive oracle proof and a (univariate) polynomial commitment. Zhang et al. instantiate this framework using Virgo, obtaining a one-to-many PCS with a prover complexity of $O(n \log n)$, as well as a verifier and communication complexity of $O(\log^2 n)$, for $n = O(d^2)$ produced proofs.

A natural application of one-to-many proofs is verifiable secret sharing (VSS) [31, 36] with low dealer complexity. VSS allows a dealer to distribute secret shares to parties so that enough honest parties could either recover the secret when the dealer is honest or identify a cheating dealer. Asynchronous VSS (AVSS) [4] operates without timing assumptions, and its resilience [1, 2] is integral for a wide array of applications, including Byzantine agreement [13], distributed key generation [19, 33], and proactive secret sharing [23, 35].

AVSS from PCS [1–3, 34] enjoys strong security guarantees (e.g., termination [18]) and low communication complexity. They roughly fall into univariate or multivariate approaches [18]. The former [34] typically adapts an encrypt-then-disperse [18] strategy to remedy any fault due to message delay or miscall. Encryption limits plaintext visibility, causing communication redundancy for sending multiple ciphertexts, and efficiency overhead for proving the well-formedness [18]. Utilizing multivariate (precisely, bivariate) PCS to build AVSS [2, 3] can achieve secret recovery and correction almost for free. A typical framework [3] involves the dealer distributing shares $f(x, y)$ of polynomial $f(X, Y)$ to party $P_i$. $P_i$ then delivers $f(x_i, y_j)$ to $P_j$, where $i, j \in \{1, 2, \ldots, n\}$. Upon receiving sufficient $f(x_i, y_j)$, $P_j$ computes $f(X, y_j)$ and sends it to $P_i$, helping it to recover or correct its share $f(x_i, Y)$. One-to-many proofs fit in nicely: a dealer proves $n^2$ different evaluations of a bivariate polynomial to $n^2$ verifiers. Each $f(x_i, y_j)$ is given to a “combined” party of $P_i$ and $P_j$.

AVSS schemes from bivariate PCS [2, 3] typically use PCS directly, leading to $O(n^3)$ dealer complexity for proving $n^2$ point evaluations on an $O(n)$-degree polynomial, each with $O(n)$ complexity. A recent work Bingo [1] reduces the dealer complexity by overloading every party with partial proof generation. The availability of one-to-many multivariate PCSs provides a potential route to lower dealer complexity. While univariate PCSs with one-to-many proofs [31, 36] exist, multivariate one-to-many proofs remain unknown. Virgo-PCS [37] (used by ZXH+22 [36]) originally supports multivariate polynomials, but it is employed in a framework solely for univariate PCS, leading to only univariate one-to-many proof.

Amidst multiple advantages, we tackle two open problems for advancing FRI-based multivariate polynomial commitments:

1. Can we build an FRI-based multivariate PCS with optimal linear proof, further with non-trivial one-to-many proof?
2. How far can we push the frontier of AVSS with the advancements in multivariate polynomial commitment?

### 1.1 Our Contribution

We solve these questions and bring the contributions below.

- **PolyFRIM**: Polynomial Commitment Scheme from Fast Reed–Solomon Interactive Oracle Proofs of Proximity in the Multivariate Setting with Linear Prover Complexity. Proving a $\mu$-variate $d$-degree polynomial at least requires its evaluation, taking $O(d^\mu)$. We propose PolyFRIM with such optimal prover complexity. Its verifier and communication take $O(\mu^2 d^2)$, living up to others [16, 37] in Table 1.

- **One-to-Many PolyFRIM**. Our new PCS design supports multivariate one-to-many proof, surpassing ZXH+22 [36] in functionality. For $O(n^2)$ proofs on any $O(n)$-degree bivariate polynomial, the prover time is $O(n^2 \log n)$, which is optimal. Per-verifier computation and communication costs stay at $O(\log^2 n)$ as the non-amortized case. Details are in Table 2.

- **FRISS**: FRI AVSS from PolyFRIM. FRISS, our new AVSS enabled by PolyFRIM (cf. [3]), exhibits a dealer complexity of $O(n^2 \log n)$ for party number $n$, the same as Bingo [1]. eAVSS [3] and HAVEN-1/2 [2] take $O(n^3)$. See Table 3. 3

- **Implementation and Evaluation**. In terms of performance, we fully implement our schemes4, which set new benchmarks. Our experiments show that PolyFRIM has 5-25× faster prover time than other transparent PCSs [11, 16, 37], with at most <30% (resp., <10%) worse verifier time (resp., proof size) compared with FRI-based PCSs. As there has been no one-to-many bivariate PCSs before, we only compare the performance of univariate one-to-many PCSs [36]. Ours reduces the prover time by 4-7× and improves the verifier time and proof size by 2-4× and 25%, respectively. For AVSS, FRISS has a 4-400× advantage for dealers on the cost of PCSs over existing schemes such as eAVSS [3] and HAVEN [2], and a 10× faster party computation than Bingo [1].

### 1.2 Technical Overview

**Contribution-I: PolyFRIM from HyperPlonk.** Succinctly, the core of HyperPlonk [16, §B] is that a $\mu$-variate multilinear polynomial $\hat{f}(X_1, X_2, \ldots, X_\mu)$ evaluated on $(x_1, x_2, \ldots, x_\mu)$ is the inner product between the coefficient vector of $\hat{f}$ and the tensor product $(1, x_1) \otimes \cdots \otimes (1, x_\mu)$. HyperPlonk primarily involves committing $\mu$ univariate polynomials $\{\hat{f}_i\}_{i \in [0, \mu-1]}$ and running the FRI low-degree test [5] for $\mu$ times to check whether $\hat{f}_i$ have respective upper degree bounds $2^{\mu-i}$.

Motivated by the demand for multivariate polynomial commitments in AVSS, we generalize HyperPlonk to cover multivariate polynomials by our dedicated transformation. This stems from the observation that a $\mu$-variable polynomial $\hat{f}(X_1, \ldots, X_\mu)$ with variable degree $d$ evaluated on $(x_1, \ldots, x_\mu)$ is equivalent to a multilinear polynomial $\tilde{g}(X_1, \ldots, X_{\log d})$

\[ \tilde{g}(X_1, \ldots, X_{\log d}) = \hat{f}(X_1, \ldots, X_\mu) \]

\[ \text{where } \hat{f}(X_1, \ldots, X_\mu) \text{ is a multilinear polynomial.} \]

\[ \text{We propose PolyFRIM with such optimal prover complexity. Its verifier and communication take } O(\mu^2 d^2), \text{ living up to others [16, 37] in Table 1.} \]

\[ \text{Per-verifier computation and communication costs stay at } O(\log^2 n) \text{ as the non-amortized case. Details are in Table 2.} \]

\[ \text{Our one-to-many bivariate PCSs before, we only compare the performance of univariate one-to-many PCSs [36]. Ours reduces the prover time by 4-7× and improves the verifier time and proof size by 2-4× and 25%, respectively.} \]

\[ \text{For AVSS, FRISS has a 4-400× advantage for dealers on the cost of PCSs over existing schemes such as eAVSS [3] and HAVEN [2], and a 10× faster party computation than Bingo [1].} \]
Table 1: Computation and communication complexities of $\mu$-variate degree-$d$ or degree-2 polynomial commitments

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Trustless Setup</th>
<th>Assumption</th>
<th>Commit</th>
<th>Prover</th>
<th>Verifier</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>PST13 [28]</td>
<td>no</td>
<td>$q$-SDH</td>
<td>$O(d^3) \mathcal{G}_B$</td>
<td>$O(d^3) \mathcal{G}_B$</td>
<td>$O(\mu) \mathcal{G}_B$</td>
<td>$O(\mu) \mathcal{G}_B$</td>
</tr>
<tr>
<td>DARK [12]</td>
<td>yes/no</td>
<td>Strong RSA</td>
<td>$O(d^2) \mathcal{G}_U$</td>
<td>$O(\mu d^2 \log d) \mathcal{G}_U$</td>
<td>$O(\mu \log d) \mathcal{G}_U$</td>
<td>$O(\mu \log d) \mathcal{G}_U$</td>
</tr>
<tr>
<td>Bulletproofs [11]</td>
<td>yes</td>
<td>DLog</td>
<td>$O(d^3) \mathcal{G}_P$</td>
<td>$O(d^3) \mathcal{G}_P$</td>
<td>$O(\mu \log d) \mathcal{G}_P$</td>
<td>$O(\mu \log d) \mathcal{G}_P$</td>
</tr>
<tr>
<td>Virgo [37]</td>
<td>yes</td>
<td>$O(\mu d^3 \log d) \mathcal{F} + O(d^3) H$</td>
<td>$O(\mu d^2 \log^2 d) \mathcal{F}$</td>
<td>$O(\mu^2 \log^2 d) H$</td>
<td>$O(\mu^2 \log^2 d) H$</td>
<td></td>
</tr>
<tr>
<td>HyperPlonk [16, SB]</td>
<td>yes</td>
<td>$O(\mu^2 d \log 2) F + O(2^\mu H)$</td>
<td>$O(\mu^2 d \log 2) F$</td>
<td>$O(\mu^2 \log^2 2) H$</td>
<td>$O(\mu^2 \log^2 2) H$</td>
<td></td>
</tr>
<tr>
<td>PolyFRIM</td>
<td>yes</td>
<td>$O(\mu d^3 \log d) \mathcal{F} + O(d^3) H$</td>
<td>$O(d^3) H + O(\mu d^3) \mathcal{F}$</td>
<td>$O(\mu^2 \log^2 d) \mathcal{F}$</td>
<td>$O(\mu^2 \log^2 d) H$</td>
<td></td>
</tr>
</tbody>
</table>

$\mathcal{G}_n, i \in \{B, U, P\}$, denotes a group with a Bilinear map, of Unknown order, or of known Prime order; $\mathcal{F}$ is a field with a large multiplicative coset. $H$ denotes a hash function. All these represent the size or operation time depending on the context.

Table 2: One-to-many proofs for $n^2$ evaluations of degree-$n$ Univariate or Bivariate polynomial commitment schemes

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Trustless</th>
<th>PCS</th>
<th>Prover</th>
<th>Verifier/Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMT [31]</td>
<td>no</td>
<td>Uni. $O(n^2 \log n)$</td>
<td>$O(\log n)$</td>
<td></td>
</tr>
<tr>
<td>ZKH$'^2$ [36]</td>
<td>no</td>
<td>Uni. $O(n^2 \log n)$</td>
<td>$O(1)$</td>
<td></td>
</tr>
<tr>
<td>ZKH$'^2$ [36]</td>
<td>yes</td>
<td>Uni. $O(n^2 \log n)$</td>
<td>$O(\log^2 n)$</td>
<td></td>
</tr>
<tr>
<td>Naive [16, 37]</td>
<td>yes</td>
<td>Bi. $O(n^2 \log n)$</td>
<td>$O(\log^2 n)$</td>
<td></td>
</tr>
<tr>
<td>PolyFRIM</td>
<td>yes</td>
<td>Bi. $O(n^2 \log n)$</td>
<td>$O(\log^2 n)$</td>
<td></td>
</tr>
</tbody>
</table>

evaluated on $(x_1^{2^d-1}, x_2^{2^d-1}, ..., x_{n}^{2^d-1})$. Such a transformation features $O(d^3)$ prover, but verifier and communication complexities are both $O(\mu^2 \log^2 d)$ for verifying $\mu$ independent proof, worse than univariate FRI-PC [32] when $\mu$ reduces to 1. Ideally, a multivariate PCS scheme should maintain the same complexity as its univariate counterpart.

Conceivably, batch-FRI [6] over a random linear combination of the $\mu$ polynomials could reduce verifier and communication complexities to $O(\mu^2 \log^2 d)$. However, while each independent proof can be tailored to a small domain, the above direct aggregation requires a single domain of an enlarged size of $O(d^3)$ to accommodate the evaluations of all polynomials $\{f_i\}_{i=0,...,\mu-1}$. The prover now takes $O(\mu d^3 \log d)$.

We propose a *rolling batch approach* to resolve the above complexity tension. It enables more efficient low-degree tests for $\{f_i\}_{i=0,...,\mu-1}$. The first round of FRI transforms $\hat{f}_0$ into polynomial $\hat{f}_0^{(1)}$ with a degree-bound of $2^{\mu-1}$, which is also the (upper) bound for the degree of $\hat{f}_1$. Generalizing our observation above, we can invoke FRI over $\hat{f}_1$, a random linear combination of $\hat{f}_0^{(1)}$ and $\hat{f}_1$ (versus independent invocations for $\hat{f}_0^{(1)}$ and $\hat{f}_1$). Similarly, we can combine every $\hat{f}_i^{(1)}$ with $\hat{f}_{i+1}$, effectively aggregating $\mu$ independent FRIs into one, yielding $O(d^3)$ prover and $O(\mu^2 \log^2 d)$ verifier/communication.

**Contribution-II: One-to-many PolyFRI**. Simplistically, producing $n^2$ proofs for degree-$n$ $f(X, Y)$ takes $n^2$ times the overhead. Merging proofs for many evaluations can be challenging. Checking the evaluation proof for bivariate $f(X, Y)$ on point $(x_i, y_j)$ takes $2 \log n = 2 \cdot t$ rounds. In the $k$-th round ($k < \log n$), the prover and verifier handle a multilinear polynomial $\hat{g}_k(x_0^0, x_1^{2^k-1}, x_0, x_1, x_2, ..., Y_1, ..., Y_{n})$ determined by $f(X, Y)$. They then transform $\hat{g}_k$ into another multilinear polynomial $\hat{g}_{k+1}(x_0^0, x_1^{2^k-1}, x_2^0, x_3^0, x_4^0, x_5, x_6, x_7, ..., Y_{n})$ instead of on $(x_0^0, x_1^0, x_2^0, x_3^0, x_4^0, x_5^0, x_6^0, x_7^0, ..., Y_{n})$. Such a transformation yields equivalence. Second, we set $x_1, ..., x_n$ as the $n$-th roots of unity $w_1, ..., w_n$, respectively, i.e., for every $i \in [n], w_i^2 = 1$, and similarly for $y_1, ..., y_n$.

Completing the whole evaluation proof can be done by constructing a binary tree of depth $2t$ as above. In the $i$-th round, the prover and verifiers would handle $2^i$ multilinear polynomials, each of size $O(n^2 \cdot 2^{i+t+1})$. The total proof complexity is reduced to $\sum_{i=0}^{t} (2^i \cdot O(n^2 \cdot 2^{i+t+1}) = O(n^2 \cdot 2^{t+1})$.

**Contribution-III: FRISS from PolyFRIM**. Synthesizing our new AVSS scheme FRISS from our one-to-many PolyFRIM is a non-trivial endeavor (i.e., our FRISS is not derived from merely black-box calling PolyFRIM) even given existing frameworks like eAVSS [3] (instantiated with KZG [24]).

Meshing PolyFRIM into AVSS is hindered by the absence of PCS homomorphism. In a typical AVSS scheme, after the dealer sends a univariate polynomial $f(x_i, Y)$ to $P_i$, $P_i$ would send $f(x_i, y_j)$ and corresponding evaluation proof $\pi_{i,j}$ to $P_j$. Some honest party $P_k$ may fail to receive valid $f(x_i, Y)$ to

---

Table 3: Existing $n$-party AVSS from multivariate PCS

<table>
<thead>
<tr>
<th>Scheme</th>
<th>PCS</th>
<th>Dealer</th>
<th>Party</th>
<th>Commun.</th>
</tr>
</thead>
<tbody>
<tr>
<td>eAVSS [3]</td>
<td>$q$-SDH</td>
<td>$O(n^2)$</td>
<td>$O(n)$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>HAVEN-1 [2]</td>
<td>$q$-SDH</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Bingo [1]</td>
<td>$q$-SDH</td>
<td>$O(n^2 \log n)$</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>HAVEN-2 [2]</td>
<td>DLog</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
<td>$O(n^2 \log n)$</td>
</tr>
<tr>
<td>FRISS</td>
<td>Ours</td>
<td>$O(n^2 \log n)$</td>
<td>$O(n^2 \log n)$</td>
<td>$O(n^2 \log^2 n)$</td>
</tr>
</tbody>
</table>

USENIX Association
33rd USENIX Security Symposium 3189
carry out secret reconstruction. To resolve this issue, after receiving sufficient evaluations and proofs, $P_j$ would compute
\[ f(X, Y) = \sum_{j=1}^{n-1} f(x_j, \pi_j) \] and send $\{f(x_j, \pi_j), \pi_{\tilde{\pi}_j}\}$ to $P_k$ to help it construct the valid $f(X, Y)$. Note that for such $P_k$, $P_j$ has to construct $\pi_{\tilde{\pi}_j}$ using $\{\pi_j\}_{j \neq k}$. The homomorphism of KZG allows such adaption of proofs for evaluation at new points, given valid proofs for $d$ evaluations of a $d$-degree univariate polynomial.

Currently, all FRI-based PCSs only use hash functions and lack homomorphism. Our solution is to let the dealer additionally send $\{f(x_j, \pi_{ij}), \pi_{\tilde{\pi}_{ij}}\}_{j \in [n]}$ to $P_i$ apart from $f(x_j, Y)$. In the reconstruction phase, $P_i$ sends $\{f(x_j, \pi_{ij}), \pi_{\tilde{\pi}_{ij}}\}$ to $P_j$. Now, even with a message delay or a malicious dealer, any honest $P_k$ can still construct valid $f(X, Y)$. Our solution increases the dealer-party communication from $O(n^2)$ to $O(n^2 \log^2 n)$ but does not affect the total complexity (as the party-party communication is already $O(n^2 \log^2 n)$). We leave it as an open problem to construct AVSS without such additional communication using bivariate PCSs without homomorphism.

1.3 Related Work

Polynomial commitment. KZG-PCS [24] achieves $O(1)$ communication and verifier complexity. It is later extended to multivariate [28]. They rely on the $q$-strong Diffie–Hellman ($q$-SDH) assumption on pairing groups and a trusted setup.

Bulletproofs [11] removes the trusted setup requirement and supports multivariate polynomials based only on the discrete-log (DLog) assumption. It uses the folding technique to achieve a proof size of $2 \log n$ group/field elements (several KBs) for polynomial size $n$. However, verification takes $O(n)$ exponentiations. Another PCS DARK [12] achieves logarithmic proof size and verification but relies on strong RSA and adaptive root assumptions. It is thus transparent only if (hence yes/no in Table 1) class groups (of a quadratic number field) are used, which are known for slower operation (e.g., [33]).

FRI-PC [5, 32], an $O(\log^2 n)$-round transparent PCS, features $O(n)$ prover and $O(\log^2 n)$ communication and verifier. It is concretely efficient, relying on field operations without exponentiations. Another PCS DARK [12] achieves logarithmic communication and verifier complexity. It is later extended to a degree-2 polynomial interactive oracle proof and can be instantiated with multivariate $\mu$-SDH assumption on pairing groups and a trusted setup.

One-to-many proofs. Tomescu et al. [31] present AMT, a one-to-many proof for KZG-PCS. It constructs an authenticated multi-point evaluation tree to compute $n^2$ evaluation proofs of a degree $O(n)$ univariate polynomial in $O(n^2 \log n)$ time. However, both communication and per-verifier complexities increase from $O(1)$ to $O(\log n)$. Zhang et al. [36] achieve a one-to-many proof for KZG with the same prover complexity without any overhead on the proof size and verifier time. Its main idea is to set the evaluation points as $n^2$-th root of unity, enabling multiple evaluations via FFT.

For transparent one-to-many proofs, Zhang et al. [36] invoke an FFT circuit using the GKR protocol [21] with $O(n^2)$ outputs such that each output is an evaluation. Notably, they propose an elegant method to unify statements for all outputs and a new Fiat–Shamir transformation so the challenges can be used for multiple verifiers. The above procedure is a polynomial interactive oracle proof and can be instantiated with any univariate polynomial commitment, but it is non-trivial to be transformed into multivariate cases due to the difficulty of constructing FFT circuits for multivariate polynomials.

AVSS. Without a synchronous network, parties cannot always receive the message from the dealer in time and may not know when all honest parties have obtained their shares to allow successful reconstruction. One recent common approach for AVSS is to rely on a bivariate polynomial to share secrets. In the sharing phase, each party receives not only its share but also pieces of shares of other parties, i.e., “share-of-share.” Parties who have received valid messages can help other parties obtain their shares by sending the pieces of other parties’ shares. eAVSS [3], employing bivariate polynomials, is the first AVSS with $O(n^2)$ communication complexity. It is also achieved by Bingo of Abraham et al. [1], an adaptively secure and optimally resilient packed AVSS. HAVEN [2] does not use bivariate polynomials but still follows the above idea using a univariate polynomial to share the secret and additional univariate polynomials to generate the pieces of parties’ shares.

Encrypt-then-disperse is an alternative [30, 34] with amortized quasi-linear communication complexity. Via asynchronous verifiable information dispersal [14] or Byzantine reliable broadcast [17], the dealer distributes an encryption of each share under each party’s key. Parties can eventually obtain their encrypted share accessible solely with their decryption key. Recently, Das et al. [18] give an AVSS with complaints, using univariate polynomials but requiring the dealer to stay online until sharing concludes.

2 Preliminaries

Notations. Let $\hat{f}(X)$ and $\hat{f}(X_1, \ldots, X_d)$ represent univariate and multivariate polynomials, respectively. Given size-$N \hat{f}$
with coefficients \((f_0, \ldots, f_{N-1})\) (low left), \(\hat{f}(X) = \sum_{i=0}^{N-1} f_i X^i\) denotes its corresponding (implicitly converted) univariate polynomial (e.g., \(\hat{f} \) and \(\hat{\hat{f}}\) in Figure 1). Let \(F\) be a prime finite field. Lowercase denotes \(F\)-elements, and bold denotes vectors on \(F\). \(x_i\) denotes the \(i\)-th entry of \(x\). \((a, b)\) and \(a \otimes b\) denote the inner and tensor product, respectively. Given a code rate \(p \in (0, 1)\) and \(L = \{\eta_1, \ldots, \eta_L\} \subseteq F^*\), an RS code \(RS[L, p] \subseteq F^L\) means \(\{\hat{f}(\eta_1), \ldots, \hat{f}(\eta_L)\} = deg(f) < p|L|\). Let \(\hat{f}_L\) be the evaluations of \(\hat{f}\) on \(L\).

We denote the security parameter by \(\lambda\), and PPT means probabilistic polynomial time. \(\text{negl}(\cdot)\) denotes a negligible function, which means for all polynomials \(\hat{f}\), \(\text{negl}(\lambda) < 1/\hat{f}(\lambda)\) for sufficiently large integer \(\lambda\). \(y \leftarrow S\) denotes picking \(y\) from set \(S\) uniformly at random. \([n] = \{1, 2, \ldots, n\}\) and \([n, m] = \{n, n+1, \ldots, m\}\) for positive integers \(m > n\).

**Merkle trees.** Merkle tree is a vector commitment with linear prover time and logarithmic verifier time and proof size, all in the vector size. It consists of three algorithms [37]. \(\rho\) code rate denotes the inner and tensor product, respectively. Given a polynomial \((\hat{f}|_{S})\) (x), \(\{\hat{f}(\eta_1), \ldots, \hat{f}(\eta_L)\}\) \(\text{deg}(f) < p|L|\). Let \(\hat{f}_L\) be the evaluations of \(\hat{f}\) on \(L\).

### Definition 2.1

\((G, P, V)\) is an interactive argument of knowledge for an NP language \(L_R\) if the following hold:

- **Completeness.** For every pp \(\leftarrow G(1^\lambda)\), every x \(\in L_R\) and \((x, w) \in R\), \(Pr[(P(w), V)\langle pp,x\rangle = 1] = 1\).
- **Argument of knowledge.** For any PPT prover \(P^{*}\), any pp \(\leftarrow G(1^\lambda)\) and any x, there is a PPT extractor \(E\) s.t. \(Pr[(P^{*}(\cdot), V^{*})\langle pp,x\rangle = 1, (x, w) \notin R\] \(\leftarrow E\langle pp,x\rangle \leq \text{negl}(\lambda)\).

### 2.1 Polynomial Commitment

**Definition 2.2.** A polynomial commitment scheme (PCS) [12, 22] for \(\mu\) variables and degree bound \(d\) is defined as follows.

- \(pp \leftarrow Gen(1^\lambda, d, \mu)\): Takes as input security parameter \(\lambda\) and bounds \(d\) and \(\mu\); generates public parameter pp.
- \(C \leftarrow \text{Commit}(pp, \hat{f})\): Takes pp and polynomial \(\hat{f}\) as input; generates the commitment C.
- \(b \leftarrow \text{VerPol}(pp, C, \hat{f})\): Verifies the opening of commitment C to the polynomial \(\hat{f}\); outputs \(b \in \{0, 1\}\).
- \(b \leftarrow \text{Eval}(pp, C, x, y, \hat{f})\): An interactive argument between a PPT prover \(P\) and verifier \(V\), which can be denoted as \(b \leftarrow \langle \text{Open}(\hat{f}), \text{Verify}\rangle\langle pp, C, x, y\rangle\). \(P\) attempts to convince \(V\) that \(\hat{f}(x) = y\). \(V\) outputs \(b \in \{0, 1\}\) at the end.

We call the prover, verifier, and communication complexity of PC the corresponding complexity of Eval, respectively.

Recent PCS definitions [22] consider completeness, polynomial binding, and knowledge soundness as necessary properties, but not zero knowledge. Zero-knowledge PCS is also not necessary for AVSS, as the secrecy only requires that parties less than the threshold cannot recover the secret instead of obtaining no additional information. Similar to HyperPlonk, our PCS is not zero knowledge, but we define a property called \(t\)-bound knowledge leaking weaker than zero knowledge (inspired by [15]), meaning that a verifier can only obtain polynomial evaluations bounded by \(t\) with no additional information. This suffices for AVSS, as shown in Section 4.

**Definition 2.3.** A multivariate PCS [22] requires:

- **Completeness.** For any polynomial \(\hat{f} \in \mathbb{F}[X]\), every pp \(\leftarrow Gen(1^\lambda, d, \mu)\), \(C \leftarrow \text{Commit}(pp, \hat{f})\) and \(\hat{f}(x) = y\), \(Pr[\text{Eval}(pp, C, r, y, x, \hat{f}) = 1] = 1\).
- **Polynomial binding.** For all pp \(\leftarrow Gen(1^\lambda, d, \mu)\), any PPT adversary \(A\), the following probability is \(\text{negl}(\lambda)\).

\[
\Pr \left[ pp \leftarrow Gen(1^\lambda, d, \mu), (C, \hat{f}_0, \hat{f}_1) \leftarrow A(pp) \right.
\overline{b_0} \leftarrow \text{VerPol}(pp, C, \hat{f}_0)
\overline{b_1} \leftarrow \text{VerPol}(pp, C, \hat{f}_1)
\left( b_0 = b_1 = 1 \right) \land \left( \hat{f}_0 \neq \hat{f}_1 \right) \right] \leq \text{negl}(\lambda).
\]

- **Knowledge soundness.** Eval is an argument of knowledge given pp \(\leftarrow Gen(1^\lambda, d, \mu)\).

\(t\)-bound knowledge leaking. For all PPT adversaries \(A\), its random tape \(r_A\), pp \(\leftarrow Gen(1^\lambda, d, \mu)\), and polynomial \(\hat{f}\), there exists a simulator \(S = (S_1, S_2)\) such that the experiments below are computationally indistinguishable, i.e., \(Pr[\text{Real}_{A, f}(pp) = 1] - Pr[\text{Ideal}_{A, S_1}(pp) = 1] \leq \text{negl}(\lambda)\).

**Theorem 2.1** ([5, 6]). FRI is an argument with soundness error \(\varepsilon_{\text{FRI}} = O(|L|/|\mathbb{F}|) + \text{negl}(q, d/|L|)\) where the verifier queries \(q = O(\lambda)\) (query repetition number) entries of every
prover’s message. The prover complexity is \(O(|L|)\) other than the \(O(|L| \log |L|)\) commitment. The verifier complexity and the communication complexity are \(O(\log^2 |L|)\).

**Batch-FRI** enables proving efficiently that \(r\) committed vectors correspond to polynomials \(f_1, \ldots, f_r\) with degree bounds \(d_1, \ldots, d_r\). Specifically, \(P\) and \(V\) invoke an FRI to check whether \(\tilde{f}|_L \in \text{RS}[L, d_{\text{max}} / |L|]\) for \(\tilde{f}(X) = \sum_{i=1}^{r} \lambda_i^{-1} \cdot \tilde{f}_i(X) \cdot X^{d_{\text{max}} - d_i}, d_{\text{max}} = \max\{d_1, \ldots, d_r\}\) and random \(A\) from \(\mathcal{V}'\).

**FRI-PC** [32]. FRI can be turned into a univariate PCS with no additional asymptotic overhead. We denote it by FRI-PC. Appendix A recalls the FRI protocol and FRI-PC.

**HyperPlonk.** HyperPlonk [16, §B], an FRI-based multilinear PCS, treats a multilinear \(\tilde{f}(x_1, \ldots, x_n)\) as the inner product of the coefficient vector of \(\tilde{f}\) and the tensor product \((1, x_1) \otimes \cdots \otimes (1, x_n)\). Theorem 2.2 (proven in Appendix B) asserts its security, which is missing in the original paper.

**Theorem 2.2.** HyperPlonk is a PCS. Its computation complexity for Commit is \(O(n \log n)\) for \(n = d\). Other complexities can be divided into two cases according to the concrete algorithm. Prover: \(O(n)\) or \(O(n \log n)\); Verifier: \(O(n \log n)\) or \(O(n \log^2 n)\); Communication: \(O(n \log^3 n)\) or \(O(n \log^2 n)\).

### 2.3 Asynchronous Verifiable Secret Sharing

An AVSS scheme consists of two phases. In the Share phase, a distinguished party called the dealer \(D\) distributes shares of a secret \(s\) to all \(n\) parties \(\{P_1, P_2, \ldots, P_n\}\) via Deal. When an honest party \(P_i\) receives a share \(s_i\) of \(s\), it completes Share. In the Reconstruction phase, any \(t + 1\) honest parties invoke a reconstruction function to recover the secret \(s\). Each party outputs \(s'\) or \(\perp\) to indicate either the successful reconstruction of the secret \(s'\) or to claim that the dealer \(D\) is malicious, respectively. Each pair of parties is connected by an asynchronous channel that provides authenticity and privacy [3]. The dealer can broadcast messages to parties by reliable broadcast [17].

Any PPT adversary \(A\) can corrupt and coordinate the actions of at most \(t\) parties. A party is honest if not corrupted. AVSS assumes no upper bound on message delivery times. \(A\) could delay messages between any two honest parties, but these messages would eventually be delivered.

**Definition 2.4** ([2, 3]). \((n, t)\)-AVSS with \(n \geq 3t + 1\) achieves:

- **Liveness.** If the dealer \(D\) is honest, all the honest parties complete the Share phase.
- **Agreement.** If some honest party completes the Share phase, then all honest parties eventually complete the Share phase. If all honest parties subsequently complete the Reconstruction phase, all honest parties complete the Reconstruction phase.
- **Correctness.** If the dealer \(D\) is honest, then the secret \(s'\) reconstructed by all honest parties equals \(s\).
- **Secrecy.** If the dealer \(D\) is honest, any PPT adversary \(A\) has no extra knowledge about \(s\).

### 3 PolyFRI with a One-to-many Prover

We first propose an FRI variant called rolling batch FRI. Section 3.2 presents an improved multilinear PCS using the rolling batch FRI, which is asymptotically better than HyperPlonk. It is then generalized to our FRI-based multivariate PCS PolyFRI in Section 3.3. Section 3.4 presents the one-to-many proofs for PolyFRI, a key component of FRISS.

#### 3.1 Rolling Batch FRI

A main overhead in HyperPlonk comes from running FRI to check every \(f_i|_{L_{i-1}} \in \text{RS}[L_{i-1}, n / |L_0|]\) for \(i \in [\mu]\), where \(L_0\) is an \(n\)-size multiplicative coset and \(L_i = \{x^2 | x \in L_{i-1}\}\).

One could run FRI for \(\mu\) times separately to complete these low-degree tests. The prover complexity is \(\sum_{i \in [\mu]} O(n/2^{i-1} \log(n/2^{i-1})) = O(n \log n)\). The verifier and communication complexities are \(\sum_{i \in [\mu]} O(n \log^2 (n/2^{i-1})) = O(n \log^2 n)\). Alternatively, a batch FRI evaluates all \(\{f_i\}_{i \in [\mu]}\) on \(L_0\). It reduces verifier and communication complexities to \(O(n \log^2 n)\) but leads to a prover complexity of \(\sum_{i \in [\mu]} O(n \log(n/2^{i-1})) = O(n^2 \log n)\) due to polynomial evaluations using FFT.

We propose rolling batch FRI (Protocol 1) to perform these \(\mu\) low-degree tests with \(O(n \log n)\) prover complexity and \(O(\log^2 n)\) verifier and communication complexities. Our high-level idea is to combine transformed polynomials during the FRI and new polynomials with the same degree to be tested. Specifically, in the \(i\)-th round of the rolling batch FRI, the current-round polynomial \(\tilde{f}(l-1)\) is transformed to a new polynomial \(\tilde{f}(l)\), which has both the same degree bound \(n/2^l\) and evaluation domain \(L_i\) as \(f_i\). So, the prover could combine \(\tilde{f}(l)\) and \(f_i\) using a random linear combination and run the FRI on a new combined polynomial. Recursively, for every \(i \in [\mu - 1]\), \(\tilde{f}(l)\) can be combined with \(f_i\), and \(\mu\) independent FRI are aggregated into one. Theorem 3.1 asserts its security.

**Theorem 3.1.** Protocol 1 is an AOk with a soundness error \(\epsilon_{\text{FRRI}} = \|L_0\| / |F|^2 + \left((1 + \rho) / 2\right)^d + \text{negl}(\lambda)\) for \(d \in (0, (1-\rho)/2)\).

The soundness of FRI comes from the correlated agreement over lines of RS code [6]: if \(u_0 + \lambda u_1\) is close to an RS codeword \(v \in \mathbb{F}[L]\), \(u_0, u_1 \in \mathbb{F}[L]\) are respectively close to two codewords with high probability for random \(\lambda\). As for rolling batch FRI, the tested vector is a random linear combination of three vectors instead of two (Steps 5 and 9, Protocol 1). Now we rely on the generalized correlated agreement over span spaces [6]: if \(u_0 + \lambda u_1 + \lambda^2 u_2\) is close to \(v\), then still with high probability \(u_0, u_1, u_2 \in \mathbb{F}[L]\) are close to three codewords, respectively. Appendix C gives the detailed proof.

**Complexity.** The prover complexity is \(O(n \log n)\) due to the FFT and Merkle tree construction for \(f_0|_{L_0}\). The computation overhead other than this is caused by FRI, where in every round, the prover computation takes \(\sum_{i \in [0,\log(n-1)]} O(n/2^i) = O(n)\). The proof size in the \(i\)-th round is \(O(q)\) field elements and \(O(\log(n/2^i))\) hashes for \(q = O(\lambda)\). The consist-
 Protocol 1 Rolling batch FRI

**Inputs:** \((\mathbb{F}, L_0, d_0); \{\hat{f}_i\}_{i \in [0, \mu - 1]}\). For \(i \in [0, \mu - 1]\), let \(d_i = d_0 \cdot 2^{i-1}\) and \(L_{i+1} = \{x^2 | x \in L_i\}\). Also, set \(n = d_0 = 2^\mu\). The prover shows \(\hat{f}_{i\mid L_i} \in \text{RS}[L_i, n/|L_0|]\).

1. For every \(i \in [0, \mu - 1]\), \(\mathcal{P}\) computes \(\hat{f}_{i\mid L_i}\), executes \(C_i \leftarrow \text{MT.Commit}(\hat{f}_{i\mid L_i})\), and sends \(C_i\) to \(\mathcal{V}\). Set \(\hat{f}(0) \leftarrow \hat{f}_0\).

2. for \(i = 1 \) to \(\mu - 1\) do

3. \(\mathcal{P}\) decomposes \(\hat{f}^{(i-1)}(X)\) into \(\hat{g}_{i}(X^2) + X \cdot \hat{h}_i(X^2)\).

4. \(\mathcal{V}\) sends \(\alpha_i \leftarrow \{\beta\} \) to \(\mathcal{P}\).

5. \(\mathcal{P}\) computes \(\hat{p}_{i}(X) \leftarrow \hat{g}_{i}(X) + \alpha_i \cdot \hat{h}_i(X)\).

6. if \(i = \mu\) then \(\mathcal{P}\) directly sends the coefficients of \(\hat{p}_{i}\).

7. else \(\mathcal{P}\) computes \(\hat{p}_{i}(0)\).

8. \(\mathcal{P}\) sends MT.Commit(\(\hat{p}_{i}(0)\)) to \(\mathcal{V}\).

9. \(\mathcal{P}\) computes \(\hat{f}(0)(X) + \alpha^2 \cdot \hat{f}_{i}(X)\).

10. for \(j = 1 \) to \(q\) do

11. \(\mathcal{V}\) sends \(\beta \leftarrow \{L_0\} \) to \(\mathcal{P}\).

12. \(\mathcal{P}\) invokes MT.Open to open \(\{\hat{f}_{i}\}, L_{i\mid}, \{\hat{p}_{i}\}, \{\mathbb{F}\}\) and \(\mathcal{V}\) checks them by MT.Verify.

13. For each \(i \in [\mu]\), \(\mathcal{V}\) checks whether the three pairs of evaluations \((\hat{f}^{(i+1)}(X^2), \hat{f}_{i}(X^2)), (\alpha_i, \hat{p}_{i}(0))\) are on a common line. Note that \(\hat{f}^{(i)}(X^2)\) can be computed by \(\hat{p}_{i}(0)(X)\) and \(\hat{f}_{i}(X^2)\).

14. Iff all the above checks pass, \(\mathcal{V}\) outputs 1; otherwise.

**HyperPlonk** achieves a succinct FRI-based multilinear PCS without proof composition (cf. [37]), but it has limitations:

1. The soundness error is directly related to the field size due to the Schwartz–Zippel lemma. Attaining the desired security level needs a large field, yet it impacts efficiency.

2. As shown in Theorem 2.2, there is a tension for HyperPlonk to achieve \(O(n)\) prover complexity, \(O(\log^2 n)\) verifier complexity, and \(O(\log^2 n)\) communication complexity.

3. The verifier may get additional knowledge from the multiple evaluations it opens on \(\{\hat{f}_i\}_{i \in [0, \mu - 1]}\), which is inapplicable to AVSS for secrecy violation, i.e., parties less than the threshold may obtain extra information about the secret.

Our proposed PCS overcomes the above limitations.

1. The verifier picks \(\beta\) from \(L_0\) instead of \(\mathbb{F}\) \(\setminus\{0\}\) and for \(i \in [\mu]\), its queries change to \(\hat{f}_{i\mid -1}(\beta^{2^{i-1}})\) instead of \(\hat{f}_{i\mid -1}(\beta)\). Now, the verifier can obtain queries by directly opening the Merkle trees instead of invoking the FRI-PC. Consequently, the prover and verifier only need to invoke the FRI to prove Equation (1) rather than the two equations below it. This avoids their computation of obtaining additional inverses of field elements and enlarging the polynomial degrees to the same. Besides, the soundness error originating from the Schwartz–Zippel lemma is no longer related to the field size.

2. Based on the idea (1), the prover now needs to show \(\hat{f}_{i\mid -1}(L_{i\mid -1}) \in \text{RS}[L_{i\mid -1}, (d_{i\mid -1} - 1)/|L_{i\mid -1}|]\) for \(i \in [\mu]\) instead of \(\hat{p}_{i\mid -1}\). This statement is exactly the same as that of rolling batch FRI in Section 3.1, and the prover and verifier can invoke the rolling batch FRI to complete these low-degree tests.

3. To mask the evaluations on \(\{\hat{f}_i\}_{i \in [\mu]}\), the prover chooses a random \(\mu\)-variate multilinear polynomial \(\bar{f}(X_1, \ldots, X_\mu)\), and sets \(f_0\) to be the univariate polynomial determined by \(\bar{f} + \alpha\bar{r}\). That is, instead of \(\bar{f}\) itself for \(\alpha \leftarrow \{\beta\}\) from the verifier. Now, the evaluations \(\{\hat{f}_i\}_{i \in [\mu]}\) are uniformly distributed because of \(\bar{r}\). Although the verifier may still obtain evaluations on \(\bar{f}|_{L_0}\), the number of leaked evaluations is limited by an upper bound, and it suffices for AVSS (in Section 4).

Below, we present 

**3.2 An Improved Multilinear PCS**

We rely on the rolling batch FRI to improve HyperPlonk. The main procedure of HyperPlonk includes: for every \(i \in [\mu]\),

1. check \(\hat{f}_{i\mid -1}(L_{i\mid -1}) \in \text{RS}[L_{i\mid -1}, (d_{i\mid -1} - 1)/|L_{i\mid -1}|]\);

2. prove the validity of \(\hat{f}_{i\mid -1}(\pm \beta), \hat{f}_i(\beta^2)\) by FRI-PC for \(\beta \leftarrow \mathbb{F}\) \(\setminus\{0\}\) from the verifier. Specifically, for each \(i \in [\mu]\), the prover \(\mathcal{P}\) proves that

\[
\hat{f}_{i\mid -1}(L_{i\mid -1}) \in \text{RS}[L_{i\mid -1}, (d_{i\mid -1} - 1)/|L_{i\mid -1}|],
\]

\[
\begin{align*}
\hat{f}_{i\mid -1}(X) - \hat{f}_{i\mid -1}(\pm \beta) & \in \text{RS}[L_{i\mid -1}, (d_{i\mid -1} - 1)/|L_{i\mid -1}|], \\
\hat{f}_{i\mid -1}(X) - \hat{f}_{i\mid -1}(\beta^2) & \in \text{RS}[L_{i\mid -1}, (d_{i\mid -1} - 1)/|L_{i\mid -1}|] (i \neq 1).
\end{align*}
\]

Here, \(d_i = d_{i-1}/2, L_i = \{x^2 | x \in L_{i-1}\}\). To prove the above three equations, for each \(i \in [\mu]\) \(\mathcal{P}\) and \(\mathcal{V}\) invoke a batch FRI to show that \(\hat{p}_{i\mid -1}(L_{i\mid -1}) \in \text{RS}[L_{i\mid -1}, (d_{i\mid -1} - 1)/|L_{i\mid -1}|]\), where \(\hat{p}_{i\mid -1}\) is a random linear combination of

\[
\begin{align*}
\hat{f}_{i\mid -1} - \hat{f}_{i\mid -1}(\pm \beta), \quad \hat{f}_{i\mid -1}(X) - \hat{f}_{i\mid -1}(\beta^2).
\end{align*}
\]
by uniquely decomposing $f_{n-1}(X)$ into $g_{n-1}(X^2) + X \cdot h_{n-1}(X^2)$. For every $i \in \{\mu - 1\}$, $P$ sets $L_i = \{x^2 | x \in L_{i-1}\}$ and sends $C_i \leftarrow \text{MT.Commit}(\hat{f}_{|L_i})$ to $\mathcal{V}'$. When $i = \mu$, $\mathcal{V}'$ can compute $\hat{f}_i = \hat{f}(x) + \alpha_1 \hat{f}(x)$ locally.

4: Set $\hat{f}(X) = \hat{f}_0(X)$. For each $i \in \{\mu\}$:
   a. $\mathcal{V}'$ sends $\hat{b}_i \leftarrow a_2 | L_0$ to $P$.
   b. $P$ derives $\hat{p}_i(X) = g_{i-1}(X) + \alpha_2 \cdot h_{i-1}(X)$ by uniquely decomposing $\tilde{f}_i(X)$ into $\tilde{g}_i(X) = \tilde{f}_i(X^2) + X \cdot \tilde{h}_i(X^2)$.
   c. $\mathcal{V}'$ runs MT.Verify to check the Merkle trees and if, $\forall i \in \{\mu\}$, triples $(\pm b^2, \pm f_i, (\pm b^2))$, $(\alpha_1 \cdot f_i, (\pm b^2))$, and $(\pm b^2, \pm \hat{t}_i, (\pm b^2))$ (note the + and − points) are on two common lines, respectively.

5: Repeat the following $q = O(\lambda)$ times:
   a. $\mathcal{V}'$ sends $\hat{b}_i \leftarrow a_2 | L_0$ to $P$.
   b. $P$ invokes MT.Open to open $\{\hat{f}_i(\pm b^2)\}_{i \in \{0, \mu - 1\}}$ and $\{\hat{p}_i(\pm b^2)\}_{i \in \{0, \mu - 1\}}$.
   c. $\mathcal{V}'$ runs MT.Verify to check the Merkle trees and if, $\forall i \in \{\mu\}$, triples $(\pm b^2, \pm \tilde{F}_i, (\pm b^2))$, $(\pm \tilde{F}_i, (\pm b^2))$, and $(\pm b^2, \pm \tilde{F}_i, (\pm b^2))$ (note the + and − points) are on two common lines, respectively.
   d. Iff all above verifications pass, $\mathcal{V}'$ outputs 1; 0 otherwise.

**Theorem 3.2.** $\mathcal{P}_{C_m}$ is a polynomial commitment scheme as described in Definition 2.3. $\mathcal{P}_{C_m}$ also has $2q$-bound knowledge leaking property. (The proof is in Appendix D.)

**Complexity.** The computation of Commit is $O(2^\mu \cdot \mu)$ due to the FFT and Merkle tree construction for $\tilde{f}_i | L_0$ and $\hat{p}_i | L_0$. As the main procedure of Eval can be seen as a tensor product argument (as in [10] and HyperPlonk) and a rolling batch FRI, the complexity overhead comes from these two protocols. The prover complexity in each round is linear to the current polynomial degree and is $\sum_{i \in \{0, \log(2\mu) - 1\}} O(2^\mu) / 2^i = O(2^\mu)$ in total. The verifier complexity and communication complexity in each round are both logarithmic to the current polynomial degree and are $\sum_{i \in \{0, \log(2\mu) - 1\}} O(2^\mu / 2^i) = O(\mu^2)$.

### 3.3 Construction of PolyFRIM

We present PolyFRIM, our multivariate PCS. Suppose $\hat{f}(x_1, \ldots, x_\mu)$ is a $\mu$-variate $d$-degree polynomial where $d = 2^\ell - 1$. Any evaluation $\hat{f}(x_1, \ldots, x_\mu)$ is equivalent to the evaluation $\hat{f}^i(x_1, \ldots, x_\mu)$, where $\hat{f}^i$ is a $\mu$-variate multilinear polynomial, and for every $i \in \{\mu\}$, $x_i = x_i^{2^\ell}$. So, the evaluation proof for $\hat{f}$ can be transformed equivalently into that for $\hat{f}^i$, which can be proved by $\mathcal{P}_{C_m}$.

The algorithms of PolyFRIM are described below.

- **pp $\rightarrow$ GenF(1^k, d, \mu):** Takes as inputs security parameter $\lambda$, degree $d$, and variable number $\mu$; outputs pp $\leftarrow$ GenF(1^k, d, \mu).
- **C $\leftarrow$ CommitF(pp, f, r):** Takes as inputs pp, polynomials $\hat{f}$ and $r$, and sets $\hat{f}$ and $r$ to be multilinear polynomials with $\mu \cdot \log(d + 1)$ variables constructed by $\hat{f}$ and $r$, respectively. The algorithm runs $C \leftarrow \text{Commit}_m(pp, \hat{f}, \hat{r})$.

- $b \leftarrow \text{VerF}(pp, C, \hat{f}, \hat{r}):$ Takes as inputs pp, $C$, $\hat{f}$, and $r$, and sets $\hat{f}$ and $\hat{r}$ be multilinear polynomials as in CommitF. The algorithm runs VerPolyF(pp, C, $\hat{f}$, $\hat{r}$, $\hat{f}$).
- $b \leftarrow \text{EvalF}(pp, C, x, y, \{\hat{f}, \hat{r}\}):$ Parse $x = (x_1, \ldots, x_\mu)$. The prover and verifier invoke the interactive argument EvalF(pp, C, $x, y$, $\{\hat{f}, \hat{r}\}$) to prove $\hat{f}'(x') = \hat{f}(x)$, where $x' = (x_1, x_2, \ldots, x_\mu)$ and for every $j \in \{\mu\}$, $x_j = (x_j^{2^0}, x_j^{2^1}, \ldots, x_j^{2^\ell})$.

**Complexity.** The complexity of PolyFRIM is similar to $\mathcal{P}_{C_m}$, but substituting the term $2^\mu$ as $d^\mu$. The time complexity of Commit is $O(\mu d^\ell \log d)$, the prover complexity is $O(d^{\ell})$, and the verifier complexity and communication complexities are $O(\mu^2 d^\ell \log d)$.

**Theorem 3.3.** PolyFRIM is a polynomial commitment scheme with $2q$-bound knowledge leaking property.

Due to the equivalence of transformation from $\hat{f}$ to $\hat{f}'$, Theorem 3.3 follows Theorem 3.2 directly.

### 3.4 Extending to One-to-many Proofs

We extend PolyFRIM for $(n, n)$-degree bivariate polynomials to one-to-many proofs with $O(n^2 \log n)$ prover complexity.

We first explain why reducing the prover complexity is challenging. When invoking PolyFRI to prove $f(x_i, y_j)$ for $i, j \in [n]$, the evaluation proof will be transformed into a proof for a multilinear polynomial on $(x_1, \ldots, x_n, y_1, \ldots, y_n)$, where $n = 2^\ell - 1$. Therefore, Equation (2) in each round is different for every verifier. Besides, the random challenges ($\alpha$ and $\alpha_1$) in Steps 3 and 4 of Protocol 1 can also be different for every verifier. Hence, the prover has to repeat PolyFRI for $O(n^2)$ times, leading to an $O(n^3 \log n)$ prover complexity.

We reduce the prover complexity by making evaluation vectors “partially the same” and random challenges “sharable” even for different verifiers. This enables the prover to save the computation overhead by reusing procedures as much as possible. The details are described below.

**Improvement on evaluation vectors.** First, we transform the evaluation vector $(x_1^{2^0}, \ldots, x_1^{2^\ell}, y_1^{2^0}, \ldots, y_1^{2^\ell})$ into its variable-inverse $(x_1^{2^{-1}}, \ldots, x_1^{2^{\ell-1}}, y_1^{2^{-1}}, \ldots, y_1^{2^{\ell-1}})$. The outcome is equivalent after reversing the order of coefficient vector $f$.

Second, we make evaluation vectors “partially the same” by picking special values for every pair $(x_i, y_j)$. This is feasible as AVSS only requires no repetition between any two distinct pairs. Specifically, for every $i, j \in [n]$, we set $(x_i, y_j) = (w_i^{2^i}, w_j^{2^j})$, where $N = n = 2^\ell$ and $w_i^{2^i}$ denotes the $z$-th root of unity. This results in only $2^k$ choices for $\{x_i^{2^i}\}_{i \in [n]}$ in the $k$-th round, i.e., the prover only needs $2^k$ operations instead of $n = 2^\ell$. The case with $Y$ is alike. The prover computation overhead related to the evaluation vector becomes $O(2 \cdot \sum_{i \in [n]} 2^k) = O(n^3 \log n)$.

**Improvement for random challenges.** We construct “shared random challenges” [34, 36] for different verifiers to make
by uniquely decomposing \( f_{k-1}^{(2,\xi_{r,k})} \) as \( g_{k-1}^{(2,\xi_{r,k})}(X^2) + X \cdot h_{k-1}^{(2,\xi_{r,k})}(X^2) \) to get \( g_{k-1}^{(2,\xi_{r,k})}(X^2) \) and \( h_{k-1}^{(2,\xi_{r,k})}(X^2) \). After the first \( r \) rounds, \( P \) will get polynomials \( f_{1}^{(2,\xi_{r,k})}, \ldots, f_{r}^{(2,\xi_{r,k})} \), corresponding to \( w_N^{(r)}, w_N^{(r)}, \ldots, w_N^{(r)} \). Here, polynomials with \( 2\xi_{r,k} \) denote the decomposition of those with \( \xi_{r,k} \).

3. The subsequent computation corresponding to variable \( Y \) is similar to Step 2. For every \( i \in [n] \), let \( f_{0}^{(i,0)} = f_{0}^{(i)} \). For every \( k \in [r] \) and \( \ell \in [0, 2^{r-1} - 1] \), \( P \) computes

\[
\begin{align*}
& f_{k+\ell}^{(i,\xi_{r,k})}(X) \leftarrow g_{k+\ell-1}^{(i,\xi_{r,k})}(X) + w_N^{\ell} \cdot h_{k+\ell-1}^{(i,\xi_{r,k})}(X), \\
& h_{k+\ell-1}^{(i,\xi_{r,k})}(X) \leftarrow g_{k+\ell-2}^{(i,\xi_{r,k})}(X) - w_N^{\ell} \cdot h_{k+\ell-2}^{(i,\xi_{r,k})}(X), \\
& C_k^{(i,\xi_{r,k})} \leftarrow MT\text{-Commit}(f_{k+\ell}^{(i,\xi_{r,k})} | L_k), \\
& C_k^{(i,\xi_{r,k})} \leftarrow MT\text{-Commit}(h_{k+\ell-1}^{(i,\xi_{r,k})} | L_k),
\end{align*}
\]

by uniquely decomposing \( f_{k+\ell}^{(i,\xi_{r,k})} \) as \( g_{k+\ell-1}^{(i,\xi_{r,k})}(X^2) + X \cdot h_{k+\ell-1}^{(i,\xi_{r,k})}(X^2) \) to get \( g_{k+\ell-1}^{(i,\xi_{r,k})}(X^2) \) and \( h_{k+\ell-1}^{(i,\xi_{r,k})}(X^2) \). \( P \) will eventually get all paths reaching all evaluation points in \( \{(w_N^{(r)}, w_N^{(r)})\}_{i,j \in [n]} \), all forking from a single root of \( f_{0}^{(i)} \).

4. For every \( i, j \in [n] \), we have commitments \( \{C_k^{(i,j,\xi_{r,k})}\}_{k \in [r]} \) and \( \{C_k^{(i,j,\xi_{r,k})}\}_{k \in [r]} \) in the path from the root \( f_{0}^{(i)} \) to the evaluation point \( (w_N^{(r)}, w_N^{(r)}) \), where \( C_k^{(i,j)} \leftarrow C_k^{(i,j) \cdot 2^r} \) and \( C_k^{(i,j,\xi_{r,k})} \leftarrow C_k^{(i,j) \cdot 2^r} \). \( P \) computes the challenge

\[
\alpha_i \leftarrow \text{H}(\alpha_i \mid \{C_k^{(i,j,\xi_{r,k})}\}_{k \in [r]} \mid \{C_k^{(i,j,\xi_{r,k})}\}_{k \in [r]}),
\]

and \( \alpha_i \leftarrow MT\text{-Commit}(\alpha_i)_{i,j \in [n]} \) in this step. Set \( \Phi_0^{(0)} = f_{0}^{(i)} \). \( P \) computes polynomials for rolling batch FRI

\[
\begin{align*}
& q_1^{(\xi_{r,k})}(X) \leftarrow g_0^{(2,\xi_{r,k})}(X) + \alpha_i \cdot h_0^{(2,\xi_{r,k})}(X), \\
& \Phi_1^{(\xi_{r,k})}(X) \leftarrow q_1^{(\xi_{r,k})}(X) + \alpha_i \cdot f_1^{(\xi_{r,k})}(X), \\
& C_1^{(\xi_{r,k})} \leftarrow MT\text{-Commit}(\Phi_1^{(\xi_{r,k})} | L_k),
\end{align*}
\]

by uniquely decomposing \( \Phi_0^{(2,\xi_{r,k})}(X) \) as \( g_0^{(2,\xi_{r,k})}(X^2) + X \cdot h_0^{(2,\xi_{r,k})}(X^2) \) to get \( g_0^{(2,\xi_{r,k})}(X^2) \) and \( h_0^{(2,\xi_{r,k})}(X^2) \). Let \( x \leftarrow (x \mod 2^r) \) for \( x \in \mathbb{Z} \). Next, for \( k \in [r] \) and \( \ell \in [0, 2^{r-1} - 1] \), \( P \) computes the Fiat–Shamir challenges

\[
\alpha_k^{(\xi_{r,k})} \leftarrow \text{H}(\alpha_k \mid C_k^{(2,\xi_{r,k})}),
\]

\[
\alpha_k \leftarrow MT\text{-Commit}(\alpha_k^{(\xi_{r,k})})_{\ell \in [0, 2^{r-1} - 1]}.
\]

Then for \( \ell \in [0, 2^{r-1} - 1] \), \( P \) computes for rolling batch FRI

\[
\begin{align*}
& q_1^{(\xi_{r,k})}(X) \leftarrow g_0^{(2,\xi_{r,k})}(X) + \alpha_k \cdot h_0^{(2,\xi_{r,k})}(X), \\
& \Phi_1^{(\xi_{r,k})}(X) \leftarrow q_1^{(\xi_{r,k})}(X) + \alpha_k^2 \cdot f_1^{(\xi_{r,k})}(X), \\
& C_1^{(\xi_{r,k})} \leftarrow MT\text{-Commit}(\Phi_1^{(\xi_{r,k})} | L_k),
\end{align*}
\]
by uniquely decomposing $\Phi_{k-1}^{(2^k)}(X)$ as $g_{k-1}^{(2^k)}(X^2) + X \cdot h_{k-1}^{(2^k)}(X^2)$ to get $g_{k-1}^{(2^k)}(X^2)$ and $h_{k-1}^{(2^k)}(X^2)$.

5. For $i \in [n]$, set $Q_i^{(0)} = \Phi^{(0)}_i$ and $C_i^{(0)} = C^{(0)}_i$. For $k \in [i], \ell \in [0, 2^k - 1 - 1]$, $P$ computes the Fiat–Shamir challenges

$$\alpha_{k+\ell}^{(i, x_{\ell})} = H(\alpha_{k, t}^{(i, x)}) || g_{k+\ell}^{(i, x_{\ell})}(1),$$

$$\alpha_{k, t}^{(i, x)} = \text{MT.Commit} \left( \{ c_{k+\ell}^{(i, x_{\ell})} \} \right)_{\ell \in [0, 2^k - 1 - 1]}.$$

Then for $\ell \in [0, 2^k - 1]$, $P$ computes for rolling batch FRI

$$Q_{k+\ell}^{(i, x_{\ell})}(X) \leftarrow g_{k+\ell}^{(i, x_{\ell})}(X),$$

$$\Phi_{k+\ell}^{(i, x_{\ell})}(X) \leftarrow \Phi_{k+\ell}^{(i, x_{\ell})}(X) + \alpha_{k+\ell}^{(i, x_{\ell})} f_{k+\ell}^{(i, x_{\ell})}(X),$$

$$C_{k+\ell}^{(i, x_{\ell})} \leftarrow \text{MT.Commit} \left( c_{k+\ell}^{(i, x_{\ell})} \right)_{k \in [n]}.$$

by uniquely decomposing $\Phi_{k+\ell}^{(i, x_{\ell})}(X)$ as $g_{k+\ell}^{(i, x_{\ell})}(X^2) + X \cdot h_{k+\ell}^{(i, x_{\ell})}(X^2)$ to get $g_{k+\ell}^{(i, x_{\ell})}(X^2)$ and $h_{k+\ell}^{(i, x_{\ell})}(X^2)$.

6. For every $i, j \in [n]$, $P$ gets $Q_{i,j} \leftarrow H(\alpha_{i,j} || C_{i,j})$ and computes $q \leftarrow \text{MT.Commit} \left( \{ Q_{i,j} \}_{i,j} \right)$ as the random evaluation set, which $P$ will open for all polynomials in $\text{Eval}_{\text{m}}$.

Every proof $\pi_{i,j}$ includes all the Merkle tree commitments, opened evaluations and their verification paths, and all verification paths for aggregated random challenges.

$P$ outputs $\text{MT.Verify}(\text{eval}_{\text{m}}, f \cdot (w_{n, w, X}^i, w_{n, w, X}^j, \pi_{i,j}))$ for $i, j \in [n]: \Psi$ uses $\text{MT.Verify}$ to check the consistency of the Merkle tree commitments against their verification paths. $\Psi$ outputs 0 if anyone fails. $\Psi$ then outputs $\text{Eval}_{\text{m}}$.Verify.

**Theorem 3.4.** The algorithm $\text{Eval}_{\text{m}}$ is a non-interactive argument for the relation $(C, x, y); f$.

From the standpoint of an individual verifier, the major distinction between $\text{Eval}_{\text{m}}$ and $\text{Eval}_{\text{STM}}$ is the random challenge generation. Instead of deriving it from the hash of preceding messages in $\text{Eval}_{\text{m}}$, $\text{Eval}_{\text{STM}}$ utilizes a Merkle tree root. This adaptation aligns with the equivalence of this mechanism to $\log N$ rounds of dummy messages [36]. The proof detailing this Fiat–Shamir transformation variant has been comprehensively addressed [36, Theorem 4].

**Complexity.** $\text{Eval}_{\text{STM}}$ computes and commits $O(2^k)$ polynomials of degree $O(2^{2k-l})$, where the evaluations of a polynomial on $L_k$ can be efficiently computed by the evaluations of polynomials on $L_{k-1}$ within $O(2^{2k-l})$ computations. So, the prover complexity is $\sum_{l \in [k]} O(2^k \cdot 2^{2k-l}) = O(t \cdot 2^k) = O(n^2 \log n)$. The communication and the verifier complexities per party are $O(\log^2 n)$, the same as PolyFRI.

### 4 Construction of FRISS

**Overview.** For threshold $t$ and $n$ parties $\{P_1, P_2, \ldots, P_n\}$, FRISS uses a $(t, t)$-degree bivariate polynomial $f(X, Y)$ to share a secret $s = f(z, 0)$ for a prescribed $z$. We set $V_{n,n} = \{(w_{n, w, X}^i, w_{n, w, X}^j, \pi_{i,j}) \}$ as evaluation points, where $n = 3t + 1$ and $N = 2^{\log n}$. On a high level, FRISS is similar with eAVSS [3] using PolyFRI instead of KZG, where the dealer firstly sends $f(x, y)$ and its commitment as the share to party $P_i$ who then sends $f(x, y_j)$ and $\pi_{i,j}$ to party $P_j$. After receiving enough evaluations and proofs, $P_j$ reconstructs $f(x, y)$ and sends $\{(x, y_j), \pi_{i,j}\}$ to $P_i$ to help $P_i$ obtain its share $f(x, y)$. However, trivially following the above idea poses challenges.

Firstly, eAVSS needs KZG to be zero-knowledge. FRISS achieves secrecy from PolyFRI’s $2q$-bound knowledge leaking by setting threshold $t = p + 2q$ for $p$ corrupted parties.

Secondly, without the homomorphism of KZG, generating $\pi_{i,j}$ for $P_j$ to aid some honest party $P_k$ to recover its share using proofs $\{(\pi_{i,j})_{i\neq j}\}$ is not straightforward. As described in Section 1.2, this can be resolved by the dealer additionally sending $\{(x, y_j), \pi_{i,j}\}_{j \in [n]}$ to $P_i$ instead of only $f(x, y)$. Thirdly, again facing the lack of homomorphism, it is unclear how to efficiently ensure the consistency among commitments to $\{(x, y)_i\}_{i \in [n]}$ and $f(X, Y)$, which is necessary for the correctness of AVSS. In a KZG-based AVSS, the dealer just broadcasts $t + 1$ commitments to $\hat{f}(x_1, y), \ldots, \hat{f}(x_{t+1}, y)$, and every party $P_i (i \notin \{i\})$ can construct the commitment to $\hat{f}(x, y)$ by homomorphism. Nevertheless, our unique construction of PolyFRI allows an almost cost-free solution. Specifically, all commitments to $\hat{f}(x, y)$ are generated from one commitment to $\hat{f}(X, Y)$, and this naturally guarantees commitment consistency. Each party needs only to use $\hat{f}(x, y)$ for an extra validity check by invoking VerPoly of FRI-PC. It is unknown how to handle this problem using other FRI-based PCSs like Virgo without such special construction.

Below, we present FRISS, consisting of Algorithms 2-4.

**Dealing phase (Algorithm 2).** Given the secret $s$, the dealer $P_d$ randomly picks $(t, t)$-degree polynomials $f(X, Y)$ and $r(X, Y)$ where $f(z, 0) = s$. $P_d$ generates proofs of $f$ and $r$ on $\text{Eval}_{\text{STM}}$. Open. In this algorithm, $P_d$ gets $\{C_i\}_{i \in [n]}$ where $C_i$ is the commitment of $f(w_{n, w, Y}^i) + \alpha \cdot \hat{f}(w_{n, w, Y}^i)$. Then $P_d$ broadcasts all the commitments and sends the Share message to $P_i$, for $i \in [n]$, which includes $\hat{f}(w_{n, w, X}^i, Y), \hat{f}(w_{n, w, Y}^i)$, and evaluations/proofs of $f$ and $r$ on $\{(w_{n, w, X}^i, w_{n, w, Y}^i)\}_{j \in [n]}$. 

Algorithm 2 Deal(s) for the dealer $P_d$

1. Sample $(t, t)$-degree polynomials $f(X, Y)$ and $r(X, Y)$ randomly, such that $f(z, 0) = s$.
2. $C \leftarrow \text{Commit}(pp, f, r); \text{frv} \leftarrow \text{pp, f, r, V}_{n,n}$.
3. $\{\langle w_{n, w, X}^i, w_{n, w, Y}^i \rangle, \hat{f}(w_{n, w, X}^i, Y), \pi_{i,j}\}_{i,j \in [n]} \leftarrow \text{Eval}_{\text{STM}}.\text{Open}(\text{frv})$.
4. For $i = 1$ to $n$ do $j \leftarrow \hat{f}(w_{n, w, X}^i, Y), \hat{P}_i \leftarrow \hat{f}(w_{n, w, Y}^i)$.
5. Broadcast $\langle \text{Commit}(C_i, \{ C_i \}) \rangle_{i \in [n]}$.
6. For $i = 1$ to $n$ do
7. For $j = 1$ to $n$ do $j, \hat{P}_j \leftarrow \hat{f}(w_{n, w, X}^i, Y), \hat{P}_j \leftarrow \hat{f}(w_{n, w, Y}^i)$.
8. Send $\langle \text{Share}, \hat{P}_j, \hat{P}_j, \{ f_{i,j}, r_{i,j}, \pi_{i,j} \} \rangle_{j \in [n]}$ to $P_i$. 

3196 33rd USENIX Security Symposium

USENIX Association
Algorithm 3 Share(_i) for party _P_i
1: if honest_dealer ← 0, sharei ← 0, echo_set ← ∅.
2: upon receiving from _P_i {Commit, _C_i, { _C_j } in [n]} and ⟨Share, _f_i, _r_i, { _f_j, _r_j, _π_j } in [n]} do
3: if Commit(pp, _f_i + α_π_i) = _C_i holds and ∀ _j ∈ [n] :
   EvalOM. Verify(pp, ( _w_N, _w_N), { _f_j, _r_j, _π_j }) then
4: honest_dealer ← 1; sharei ← _f_i.
5: Send ec_i,j = ⟨Echo, _f_j, _r_j, _π_j⟩ to _P_j, ∀ _j ∈ [n].
6: upon receiving ec_i,j from _P_j for the first time do
7: if EvalOM. Verify(pp, ( _w_N, _w_N), { _f_j, _r_j, _π_j }) then
8: Mark Echo as valid.
9: echo_set ← echo_set ∪ { ( _w_N, _w_N), { _f_j, _r_j, _π_j }}.
10: upon getting 2r + 1 valid Echo & honest_dealer = 1 do
11: Send ⟨Ready⟩ to all parties.
12: upon receiving t + 1 Ready and not yet sent Ready do
13: Send ⟨Ready⟩ to all parties.
14: upon receiving 2r + 1 Ready do
15: Wait until t + 1 valid Echo.
16: Interpolate _f_i and _r_i using the set echo_set.
17: output sharei ← _f_i and terminate.

Sharing phase (Algorithm 3). Honest party _P_i first checks the correctness of _C_i, then checks if the received evaluations are valid by EvalOM. Verify. If all the verifications pass, _P_i will set honest_dealer = 1, and send an Echo message with _f( _w_N, _w_N), its proof, and _r( _w_N, _w_N) to other parties. Through a typical “Echo + Ready” approach [2] (Steps 6-16, Algorithm 3), a party who has not received the Share message will get its share by t + 1 valid Echo messages. When Share terminates, _P_i gets _f_N( _w_N, _Y) as its share.

At the end of the Share phase, every honest party receives at least 2r + 1 valid Echo messages. At least t + 1 of them are sent by honest parties with honest_dealer = 1. Further, every such honest _P_i has a valid commitment _C_i and valid polynomial _f_N( _x, _Y), so is able to generate a valid proof for _f_i(0).

Reconstruction phase (Algorithm 4). Every (at least t + 1) honest _P_i with honest_dealer = 1 sending _f_i(0) and corresponding proof to other parties would suffice to recover the secret. However, at most t honest parties with honest_dealer = 0 could not participate in the reconstruction as they cannot generate valid proofs. We propose an alternative to enable these “weaker” parties to contribute to the reconstruction.

Specifically, if _P_i is with honest_dealer = 1, it would send Rec_strong, evaluations, and corresponding proof to other parties. Otherwise, it just sends Rec_weak and evaluations. For another honest party _P_j, if it receives at least t + 1 proofs, it can verify the validity of evaluations and get its share directly by interpolation. If it receives sufficient evaluations (some with proofs but less than _t and some without), it can still compute _f_N( _x, 0) by an efficient RS decoding algorithm such as Berlekamp–Welch, hence computing _f_N( _z, 0).

Algorithm 4 Reconstruction_i() for party _P_i
1: if honest_dealer = 1 then
2: _π_i ← Eval.Open(pp, _C_i, _f_i + α_π_i, 0).
3: Send _r_i = ⟨Rec_strong, _f_i(0), _r_i, _π_i⟩ to all parties.
4: if honest_dealer = 0 then
5: Send _r_i = ⟨Rec_weak, _f_i(0), _r_i(0)⟩ to all parties.
6: upon receiving _r_i for the first time do
7: if Eval.Verify(pp, _C_j, _f_i(0) + α_π_j, 0) then
8: valid_rec ← valid_rec ∪ { _f_i(0) }.
9: decode_set ← decode_set ∪ { _f_i(0) }.
10: if |valid_rec| ≥ t + 1 then
11: Get _f_N( _x, 0) by interpolation and obtain _f_N( _z, 0).
12: terminate.
13: upon receiving _r_i from _P_j for the first time do
14: decode_set ← decode_set ∪ { _f_i(0) }.
15: if |decode_set| ≥ 2|valid_rec| ≥ 3t + 1 then
16: Get _f_N( _x, 0) by decoding and obtain _f_N( _z, 0).
17: terminate.

Theorem 4.1. FRISS is an (n, t)-AVSS scheme as in Definition 2.4. Appendix E provides a formal proof.

Complexity. The dealer complexity mainly comes from generating proofs in Step 3. Algorithm 2 using the one-to-many PolyFRI, which is _O(n^2 log n) as _t = _O(n), _N = _O(n).

The per-party computation overhead comes from:
1 verifying proofs for _O(n) times using EvalOM. Verify in Steps 3 and 7, Algorithm 3: _O(n) · _O(log^2 n) = _O(n log^2 n);
2 generating proofs using the FRI-PC Eval algorithm in Step 3, Algorithm 4: _O(n);
3 verifying proofs for _O(n) times by the FRI-PC Verify algorithm in Step 8, Algorithm 4: _O(n) · _O(log^2 n) = _O(n log^2 n).

So, the per-party computation overhead is _O(n log^2 n).

The communication overhead comes from:
1 the dealer sending shares and proofs in Step 8, Algorithm 2: _O(n^2) + _O(n^2) + _O(log^2 n) = _O(n^2 log^2 n);
2 the dealer broadcasting commitments in Step 5, Algorithm 2: _O(n^2) using reliable broadcast (e.g., [14]);
3 party sending shares and proofs in Step 5, Algorithm 3 and Step 4, Algorithm 4: _O(n^2) · _O(log^2 n) = _O(n^2 log^2 n).

So, the total communication complexity is _O(n^2 log^2 n).

5 Empirical Conclusion

We wrote ~1,600 lines for PolyFRI and ~1,800 lines for FRISS in Rust. We ran all experiments on an AMD Ryzen 3900X processor with 80GB RAM and Ubuntu 22.04 LTS operating system. Reported figures are averages over 10 executions. We assume no parallelization.

We use _F_p^2 as our field, _p = 2^64 – 1 [37], with a multiplicative cost of size up to _2^60. For all FRI-based schemes (Virgo [37],
As shown, for size being 2\textsuperscript{100} bits of security [6, Conjecture 8.4]. Besides, we committed domain. Its smaller proof size is due to the rolling FRI-PC by changing the queries from the whole field to the degree by half in each round. Our hash function is blake3.\textsuperscript{3}

5.1 Performance of PolyFRIM

We compare PolyFRIM with other transparent PCSs, including Bulletproofs \textsuperscript{[11]}\textsuperscript{6}, Virgo \textsuperscript{[37]}\textsuperscript{7}, and HyperPlonk \textsuperscript{[16]}. As HyperPlonk is not open-sourced, we implement it ourselves.

Figure 2 shows their prover time, verifier time, and proof size. The size of the multivariate polynomial (number of monomials) varies from 2\textsuperscript{5} to 2\textsuperscript{20} (as in [36]). We run out of memory for HyperPlonk when the polynomial size is 2\textsuperscript{19}. As shown, for size being 2\textsuperscript{20}, the prover time of PolyFRIM takes only 4.4s, which is 6×, 10×, and 25× faster than Virgo, HyperPlonk, and Bulletproofs, respectively.

PolyFRIM has a 4-10× faster verifier and a 2-3× smaller proof size than HyperPlonk. This speed stems from avoiding FRI-PC by changing the queries from the whole field to the committed domain. Its smaller proof size is due to the rolling batch FRI, which reduces Merkle tree depth and verification path size. The verifier time and proof size of PolyFRIM are competitive with Virgo (less than 50% and 10% worse, respectively). As for Bulletproofs, PolyFRIM has a 100-200× larger proof size but can be 1000× faster for verification.

5.2 Performance of One-to-Many PolyFRIM

PolyFRIM is the first multivariate PCS with one-to-many proof. Figure 3a shows the prover time. One-to-many PolyFRIM is 800-10\textsuperscript{9}× faster than its trivial repetition. It only takes 0.07s (resp., 49.4s) to generate 2\textsuperscript{12} (resp., 2\textsuperscript{20}) proofs for a 2\textsuperscript{12}-degree (resp., 2\textsuperscript{20}-degree) polynomial. Using only lightweight crypto operations (RS codes and hash), our prover time is 25-100× and 10\textsuperscript{3}-10\textsuperscript{9}× faster than AMT\textsuperscript{8} and KZG, respectively. For one-to-many ZXH\textsuperscript{22}, our prover time is 4-7× faster for eliminating the need for the GKR protocol [21,36] (and PolyFRIM is faster than Virgo).

As in Figure 2b, our per-verifier time is 3-9× (resp., 2-4×) faster than AMT (resp., ZXH\textsuperscript{22}). Even compared with constant-verifier KZG, ours is concretely faster for n < 2\textsuperscript{14}.

Figure 2c shows the proof size. Ours is larger than trusted-setup-based AMT and KZG. PolyFRIM features up to 20%
smaller proof size than transparent ZXH+22, thanks to its avoidance of additional GKR protocol for delegation.

### 5.3 Performance of PolyFRIM in AVSS

Figure 4 compares the performance of PCSs in different AVSS schemes (eAVSS [3], HAVEN [2], and Bingo [1]) for varying numbers of parties $n = 3t + 1$ and degree-$t$ polynomials.

For FRISS, the dealer generates $n^2$ proofs for a $(t, t)$-degree polynomial using PolyFRIM, and each party verifies $n$ proofs. In eAVSS and HAVEN, everything is the same except using different PCSs (KZG for eAVSS and HAVEN-1, and Bulletproofs for HAVEN-2). Following these works, we achieve a bivariate KZG by committing $n$ degree-$t$ univariate polynomials and generating $n$ proofs for every polynomial. For Bingo, the dealer just commits $t + 12r$-degree univariate polynomials, and every party generates $n$ proofs for a $2r$-degree univariate polynomial using KZG.

Figure 4 shows the generation time of commitments and evaluation proofs for the dealer (Steps 2-3 in Algorithm 2) and verification time (Steps 3 and 7 in Algorithm 3) for every polynomial. We omit PCS-irrelevant parts (e.g., broadcast/encryption) to focus on how PCS improves AVSS. The dealer time of FRISS caused by the PCS is $4-800\times$ faster than AVSS using a similar method (eAVSS and HAVEN-1/2). Our per-party time is $0.5-1.2\times$ of eAVSS and HAVEN-1. In Bingo, proof generation is partially “shifted” from the dealer to the parties, so FRISS is $10\times$ slower for the dealer but $10\times$ faster for parties.

### References


A The FRI Protocol and FRI-PC

Protocol 5 The FRI protocol to test if $\hat{f}_L \in RS[L, d/|L|]$

\begin{itemize}
  \item \textbf{Inputs:} (($F, L, d), (f)$). $L$ is a multiplicative coset. Without loss of generality, we assume $d = 2^r$ for a positive integer $r$.
  \item \textbf{1:} $P$ sets $L_0 = L$, $\hat{f}_0 = \hat{f}$, computes $f_0_{|L_0}$, executes $r_0 \leftarrow MT.\text{Commit}(f_{0_{|L_0}})$, and sends $r_0$ to $\mathcal{V}'$.
  \item \textbf{2:} for $i = 1$ to $r + 1$
    \begin{itemize}
      \item $\mathcal{P}$ decomposes $\hat{f}_{i-1}$ as $\hat{g}_i(X^2) + X \cdot \hat{h}_i(X^2)$.
      \item $\mathcal{V}'$ sends $\alpha_i \leftarrow q \mathbb{F}$ to $\mathcal{P}$.
      \item $\mathcal{P}$ computes $\hat{f}_i(X) = \hat{g}_i(X) + \alpha_i \cdot \hat{h}_i(X)$.
      \item If $i \neq r + 1$, $\mathcal{P}$ computes $\hat{f}_{i_{|L_i}}$ where $L_i = \{x^2 | x \in L_{i-1}\}$, runs $r_t \leftarrow MT.\text{Commit}(\hat{f}_{i_{|L_i}})$, and sends $r_t$ to $\mathcal{V}'$.
      \item If $i = r + 1$, $\mathcal{P}$ directly sends $f_i$ to $\mathcal{V}'$.
      \item for $j = 1$ to $q = O(\lambda)$
        \begin{itemize}
          \item $\mathcal{V}'$ sends $\beta \leftarrow q \mathbb{F}$ to $\mathcal{P}$.
          \item $\mathcal{P}$ uses $MT.\text{Open}$ to open $\hat{f}_{i-1}(\pm \beta^{2^{r-1}}, \hat{f}_i(\beta^2))$.
          \item $\mathcal{V}'$ checks the correctness by $MT.\text{Verify}$.
          \item $\mathcal{V}'$ checks if the pairs $(\pm \beta^{2^j}, \hat{f}_{i-1}(\pm \beta^{2^j}))$ are on a common line.
      \end{itemize}
      \item If all the above checks pass, $\mathcal{V}'$ outputs $1$; $0$ otherwise.
    \end{itemize}
\end{itemize}

We recall FRI in Protocol 5, and FRI-PC below.

- $pp \leftarrow \text{Gen}(1^k, d)$: Takes as inputs the security parameter $k$ and the degree bound $d$; outputs public parameter $pp$, which includes the field $\mathbb{F}$ and a multiplicative coset $L$.
- $C \leftarrow \text{Commit}(pp, \hat{f})$: Executes $C \leftarrow MT.\text{Commit}(\hat{f}_{|L})$. 

---


[34] Thomas Yurek, Licheng Luo, Jaiden Fairoze, Aniket Kate, and Andrew Miller. hBACSS: How to robustly share many secrets. In NDSS, 2022.


There exists some $\hat{C}$ such that $\hat{f} \cdot \hat{f}' \cdot \hat{f}^4$: For every $i \in \mathbb{X}$, suppose $\hat{C}$ and $\hat{f}$ are consistent. Let $\mathbf{pp} \leftarrow \text{Gen}(\mathbf{C}, \hat{f})$: Takes as inputs $\mathbf{C}$ and a variable number $\mu$, outputs public parameter $\mathbf{pp}$ publicly. Let $\mathbf{C} \leftarrow \text{Gen}((\mathbf{C}, \hat{f}))$: Takes as inputs $\mathbf{C}$ and $\hat{f}$, outputs the commitment $\mathbf{C} \leftarrow \text{Gen}(\mathbf{pp}, \hat{f})$. Let $\mathbf{pp} \leftarrow \text{Gen}(\mathbf{C}, \hat{f})$: Runs VerPoly$(\mathbf{pp}, \mathbf{C}, \hat{f})$, generating a variable number $\hat{C}$. Let $\mathbf{pp} \leftarrow \text{Gen}(\mathbf{C}, \hat{f})$: Runs VerPoly$(\mathbf{pp}, \mathbf{C}, \hat{f})$. Let $\mathbf{pp} \leftarrow \text{Gen}(\mathbf{C}, \hat{f})$: Runs VerPoly$(\mathbf{pp}, \mathbf{C}, \hat{f})$.

Suppose Equation (3) holds when $i = k$, and we next prove Equation (3) also holds when $i = k + 1$. Since $\hat{f}_i(X) = \hat{f}_E^{(k+1)}(X^2) + X \cdot \hat{f}_O^{(k+1)}(X^2)$, we have

$$\hat{f}_E^{(k+1)}(X^2) = \sum_{j \in [0,2^m-1], j_k = 0} a_j x_1^j \cdots x_{k-1}^j X^{2j+2 \cdots 2^{m-1} - j_k},$$

$$\hat{f}_O^{(k+1)}(X^2) = \sum_{j \in [0,2^m-1], j_k = 1} a_j x_1^j \cdots x_{k-1}^j X^{2j+2 \cdots 2^{m-1} - j_k}.$$

We thus have $\hat{f}_{k+1}(X) = \hat{f}_E^{(k+1)}(X) + x_{k+1} \cdot \hat{f}_O^{(k+1)}(X)$ by the procedure of HyperPlonk, then we have $\hat{f}_{k+1}(X)$ equals to $\sum_{j \in [0,2^m-1]} a_j x_1^j \cdots x_{k+1}^j X^{(j+1)+2 \cdots 2^{m-1} - j_{k+1}}$. So, Equation (3) holds for all $i \in [0, \mu]$.

To see $\hat{f}_\mu(\pm \beta) = y$, we show by induction that $\hat{f}_\mu(\pm \beta)$ equals to $\sum_{j \in [0,2^m-1]} a_j x_1^j \cdots x_{\mu}^j = (\hat{f} (1, x_1) \otimes \cdots \otimes (1, x_\mu)) = y$.

Besides, for every $i \in [0, \mu]$, $\hat{f}_i(X) \leftarrow \hat{f}_E^{(i)}(X) + x_i \cdot \hat{f}_O^{(i)}(X)$, where $\hat{f}_E^{(i)}(X^2) = (\hat{f}_E^{(i-1)}(X) + \hat{f}_E^{(i-1)}(-X))/2$ and $\hat{f}_O^{(i)}(X^2) = (\hat{f}_O^{(i-1)}(-X) - \hat{f}_O^{(i-1)}(-X))/2$. Hence $\hat{f}_i(\beta) = (\hat{f}(\beta) + \hat{f}(-\beta))/2 + x_i (\hat{f}(\beta) - \hat{f}(-\beta))/\beta$.

**Polynomial binding.** For proximity parameter $\delta \leq (1-\rho)/2$, by the soundness of batch FRI, if the verifier accepts in VerPoly, with probability $1 - \text{neg}(\lambda)$ each opened vector of commitment binds to the encoding of a unique univariate polynomial. The polynomial binding property hence follows.

**Soundness.** Suppose that $\hat{f}(x_1, \ldots, x_\mu) \neq y$, and $\hat{f}_1, \ldots, \hat{f}_\mu$ are actually committed polynomials. We argue by two cases:

- **Case 1.** There exists some $\hat{f}_i$ for $i \in [0, \mu - 1]$ of degree at least $2^{m-i}$ or the evaluation proof for $\hat{f}_i$ is invalid. According to Theorem 2.1, this probability is at most $\varepsilon_{\text{FRI}}$.

- **Case 2.** Degrees of $\{\hat{f}_i\}$ are less than $2^{m-i}$ for $i \in [0, \mu]$ and the evaluation proofs are all valid. Since $\hat{f}(X) \neq y$, there must be some $i$ such that $\hat{f}_i(X) \neq \hat{f}_E^{(i)}(X) + x_i \cdot \hat{f}_O^{(i)}(X)$ but it holds for all queries. Assume $j$ is the smallest of such $i$. By definition, $\hat{f}_E^{(j)}(X^2) = (\hat{f}_j(\beta) + \hat{f}_j(-\beta))/2$, and $\hat{f}_O^{(j)}(X^2) = (\hat{f}_j(\beta) - \hat{f}_j(-\beta))/2$. Set $\hat{g}(X)$ to be:

$$\hat{g}(X^2) = \frac{\hat{f}_j(\beta) + \hat{f}_j(-\beta) - 2\hat{f}_j(X)}{2\beta}.$$

$\hat{g}(X)$ is a non-zero polynomial with a degree at most $2^{m-j} - 1$, so the soundness error is bounded by $2^{m-j+1}/|\mathbb{F} \setminus \{0\}| \leq 2^{m}/|\mathbb{F} \setminus \{0\}|$ according to the Schwartz–Zippel lemma.

Using the union bound argument, the total soundness error of HyperPlonk is $\varepsilon_{\text{FRI}} + 2^{m}/|\mathbb{F} \setminus \{0\}|$. By appropriate parameter choices for $\mathbb{F}$, $L$, and $\mu$, the soundness error can be negligible.

**Knowledge soundness.** HyperPlonk is an argument of knowledge with extractability of Merkle trees proven in the random oracle model [8, 37]. Roughly, given the root and sufficiently many authentication paths, there exists an efficient extractor that reconstructs the leaves with high probability. Additionally, the leaves are RS codewords and can be efficiently decoded by decoding algorithms such as Berlekamp–Welch.
Specifically, for any PPT adversary $P_0$ with Commit$^*$ and Eval$^*$, there exists a PPT extractor $E$ such that given the random access tape of $P_0^*$, the following probability is $\negl(\lambda)$:

$$\Pr \left[ C^* \leftarrow \text{Commit}^*(pp, \tilde{f}^*), \tilde{f}^* \leftarrow E(pp, C^*, x, y^*), \; 1 \leftarrow \text{Eval}^*(pp, C^*, x, y^*, \tilde{f}^*), \; y^* \neq \tilde{f}^*(x) \right] \right].$$

Suppose the Merkle tree is based on a random oracle $H : \{0,1\}^{2\lambda} \rightarrow \{0,1\}^{\lambda}$. We then construct a PPT extractor $E$ with the same random type of $P_0^*$ working as follows:

1. $E$ mirrors the process of $P_0^*$ querying $H$. Let the queries made by $P_0^*$ to $H$ be $(q_1, q_2, \ldots , q_{\text{max}})$ in the order they are made with duplicates excluded, which implies that queries are not generated from parent nodes to child ones.

Define $q_j \in H(q_j)$ if the first $\lambda$ bits or the last $\lambda$ bits of $q_j$ is $H(q_j)$, i.e., $q_j$ could be the parent node of $q_j$. If there exists some $i \neq j, H(q_i) = H(q_j)$ or some $i \leq j, q_j \in H(q_j)$, $E$ outputs random polynomial $\tilde{f}$ and aborts; otherwise we suppose that $H(q_j) = C^*$ for some $r$.

If any verification path is invalid, $E$ outputs a random polynomial $\tilde{f}$ and aborts.

2. $E$ constructs a directed graph $G$ according to the query set $Q = \{ q_1, q_2, \ldots , q_{\text{max}} \}$. There is an edge from $q_j$ to $q_i$ in $G$ if and only if $q_j \in H(q_i)$, i.e., the outdegree of each node is at most 2. When $P_0^*$ generates $C^*$ in the Commit$^*$ algorithm, if $C^*$ does not equal $H(q_j)$ for some $q_j \in Q$ with depth $[\mu]$, the binary tree, $E$ outputs a random polynomial $\tilde{f}$ and aborts; otherwise we suppose that $H(q_j) = C^*$ for some $r$.

If any verification path is invalid, $E$ outputs a random polynomial $\tilde{f}$ and aborts.

3. $E$ reads all leaves from the root $q_r$. If there exists any missing leaf, $E$ outputs a random $\tilde{f}$ and aborts; otherwise, it concatenates these leaf strings and decodes the string using an efficient RS decoding algorithm. Therefore, $E$ could efficiently output the coefficients of $\tilde{f}$.

Let $E_1$ be the event $\psi'$ accepts, and $E_2$ be $y^* \neq \tilde{f}(x)$. Consider $\Pr[E_1 \land E_2]$. Suppose that $E$ aborts before constructing the graph $G$. If for some $i \neq j, H(q_i) = H(q_j)$, $E$ finds a collision. If for some $i \leq j, q_j \in H(q_i)$, $E$ could generate a Merkle tree violating the logical order. Either probability is $\negl(\lambda)$ since $H$ is collision-resistant and non-invertible.

Otherwise, $E$ has successfully constructed a graph $G$. If some node on a verification path does not lie in $G$, $P_0^*$ has to guess the value to construct a valid verification path, and this probability is $\negl(\lambda)$ since $H$ is non-invertible. Additionally, if any leaf is missing, $\psi'$ will be convinced with probability $\negl(\lambda)$ once it queries this leaf. The probability that this leaf is not queried by $\psi'$ is at most $(1 - 1/|L_0|)^{\alpha} = \negl(\lambda)$ as the query repetition number of FRI-PC $q$ satisfies $q = O(\lambda)$. If $E$ does not abort, it could always efficiently extract the coefficient vector of $\tilde{f}$. In this case, $\psi'$ accepts the statement with probability $\negl(\lambda)$ with an appropriate choice of parameters according to the soundness. So, we can bound $\Pr[E_1 \land E_2]$:

$$\Pr[E_1 \land E_2 | \text{E aborts}] + \Pr[E_1 \land E_2 | \text{E does not abort}] \leq \Pr[\text{E aborts}] + \Pr[E_1 \land E_2 | \text{E does not abort}] \leq \negl(\lambda).$$

**Complexity.** Commit takes $O(n \log n)$, mainly caused by the FFT operation and the construction of the Merkle tree for $\tilde{f}_L$. The other complexities depend on the concrete algorithm.

- **Case 1.** The prover shows that $\{ \tilde{f}_1(\pm \beta) \}$ is valid round by round independently. The prover complexity is $\sum_{i \in [\log n]} O(n/2^i) = O(n)$. The verifier and communication complexities are both $\sum_{i \in [\log n]} O((n/2^i))^2 = O(n^2)$. 

- **Case 2.** The prover invokes a batch FRI to prove the validity of all the evaluations, where all $\{ \tilde{f}_i \}_{i \in [\mu]}$ are computed and evaluated on the same multiplicative coset. The prover complexity is hence $O(n \log n)$ caused by constructing Merkle trees for $\log n$ n-length vectors. The verifier and communication complexities are both $O(\log^2 n)$ due to the batch FRI. 

\[
\square
\]

**C Proof of Theorem 3.1**

**Proof.** The completeness comes directly from that of the FRI protocol. Similar to the proof in Appendix B, the argument of knowledge property holds according to the extractability of Merkle trees. We mainly prove the soundness property below from the following two cases.

- **Case 1.** If any of the Merkle tree commitments $\{ \pi_x \}_{x \in \{0,1\}^{\mu}}$ is not valid, or the leaves are inconsistent with the roots, the verification passes with probability no more than $\negl(\lambda)$.

- **Case 2.** All the Merkle tree commitments are valid, and the leaves are consistent with corresponding roots. For this case, we first define functions $\{ \back(A) \}_{A}$ and sets $\{ \err(A) \}_{A}$.

Define $\back(A) = A_{00} \land A_{11}$. For $A_{00} \land A_{11}$, and $\back(A) = \back(A_{00} \land A_{11}) = A_{10} \land A_{11}$. Define $\err(A) = \err(A_{10} \land A_{11})$.

For $i \in [\mu]$, let the set $E_i = \{ x \in E_{i-1} : \tilde{g}_i(x^2) + \alpha \tilde{h}_i(x^2) + \alpha^2 \tilde{f}_i(x^2) \neq \tilde{f}_i(x^2) \}$, where $\tilde{f}_i(x^2) = \tilde{g}_i(x^2) + X \cdot \tilde{h}_i(x^2)$. Define $\err_i = \err(E_{i-1} \land \back(E_{i-1})$.

By $i \in [\mu]$, suppose that $\tilde{h}_i(x) \in \text{RS}[\lambda, \rho]$ and set $A_0 = \{ x \in E_i : \tilde{f}_i(x) = \tilde{h}_i(x) \}$. Define $\err(A_{00} \land A_{11}) = \err(A_{0} \land A_{11}) / |L_0| = (\lambda - 1) / |L_0|$. By the union bound argument, the total soundness error is $|L_0|/|F| + (\lambda - 1) / |L_0| \leq \negl(\lambda)$.

To prove Inequality (4), we first describe three lemmas.

**Lemma C.1 (6).** For $\delta < (1 - \rho)/2$, $\tilde{f}_{i \in [\mu]}$ with degree bounds $d$ and multiplicative coset $L$ where $\rho = d/|L|$, if

$$\Pr[ \sum_{i=0}^{n-1} \alpha \cdot \tilde{f}_{i} L, \text{RS}[L, \rho] \leq \delta \geq |L|/|F|,$$
where $\Delta(a, b)$ is the relative Hamming distance between $a$ and $b$, there exists $L' \subseteq L$ and $\hat{\rho}_0, \ldots, \hat{\rho}_{n-1}$ with degree bound $d$ such that $|L'|/|L| \geq 1 - \delta$ and $\hat{f}_i|_{L'} = \hat{\rho}_i|_{L'}$ for $i \in [0, n-1]$.

**Lemma C.2.** For any $S_1 \subseteq S_2 \subseteq L$, $\epsilon_i(S_1) \geq \epsilon_i(S_2)$.

**Proof.** By definition, $\epsilon_i(S_1) - \epsilon_i(S_2) = (|S_2| - |S_1|) - (|\text{back}(S_2) \cap \text{err}_i| - |\text{back}(S_1) \cap \text{err}_i|)/|L| = |S_2 \setminus S_1|/|L| - |\text{back}(S_2) \setminus \text{back}(S_1)|/|\text{back}(L)| = |\text{back}(S_2 \setminus S_1)|/|\text{back}(L)| \geq 0$.

**Lemma C.3.** For every $i \in \alpha$ and $\hat{h}_i = RS(L, \rho)$, if $\Delta(\hat{\rho}_i|_{L} + \rho_i, \hat{\rho}_i|_{L}) \geq \delta$, then $\epsilon_i(A_i) \geq \delta$.

**Proof.** Let $\hat{f}_i - f_i + \hat{\rho}_i$ and $\hat{\rho}_i + \hat{\rho}_i f_i$. Define set $B = A_i \cup \{x \in L_s \mid \hat{f}_i(x) \neq f_i(x)\}$. Define polynomial $\hat{f}_i$ such that $\hat{f}_i(x) = \hat{h}_i(x)$ when $x \in B$ and $\hat{f}_i(x) = f_i(x)$ when $x \notin B$.

For all $x \in B$, $\hat{f}_i(x) = f_i(x)$ because $\hat{h}_i(x)$ is the number of points in $B$ which is not less than the Hamming distance between $\hat{f}_i(x)$ and $f_i(x)$, i.e., $\hat{f}_i(B) \cap \text{err}_i(x)|/|L_x| \geq \Delta(\hat{f}_i(x), \hat{h}_i(x))$. Also, $\hat{f}_i(x) = \hat{h}_i(x)$ holds for all $x \in B$, $1 - |B|/|L| \geq \Delta(\hat{f}_i(B), \hat{h}_i(B))$. So, $\epsilon_i(B) = \Delta(\hat{f}_i(x), \hat{h}_i(x)) \geq \Delta(\hat{f}_i, \hat{h}_i)|\alpha_i| \geq \delta$. Therefore, below we only need to consider the following case:

**Proof of Inequality (4).** We prove by induction. When $\mu = 1$, Protocol 1 is a standard FRI, and soundness holds naturally. If Inequality (4) holds for $\forall \mu < t$, we show it holds for $\mu = t + 1$.

When $\mu = t$, the protocol can be seen as a partial protocol starting from $\hat{f}_i(x) = f_i(x)$ for $\mu = t + 1$. By induction, when $\mu = t + 1$, the following holds:

- If there exists $i \geq 1$, such that $\Delta(f_i(x), RS(L, \rho)) \geq \delta$, then $\Pr(\epsilon_i(A_i) \geq \delta) \geq 1 - |\text{back}(B)|/|\text{back}(L)|$.
- If there exists $i \geq 2$, such that $\Delta(\hat{f}_i(B), RS(L, \rho)) \geq \delta$, then $\Pr(\epsilon_i(A_i) \geq \delta) \geq 1 - |\text{back}(B)|/|\text{back}(L)|$.

Therefore, we only need to prove Inequality (4) in the following case: (a) For all $i \geq 1$, $\Delta(f_i(x), RS(L, \rho)) \leq \delta$; (b) For all $i \geq 2$, $\Delta(\hat{f}_i(x), RS(L, \rho)) \leq \delta$; (c) At least one of $\Delta(f_i(x), RS(L, \rho)) \geq \delta$ and $\Delta(\hat{f}_i(B), RS(L, \rho)) \geq \delta$ holds.

As (3) holds, there does not exist $A_i \subseteq L_1$ and $A_i \setminus |\text{back}(B)| \geq 1 - \delta$ such that $\hat{g}_i|_{L_1}, \hat{h}_i|_{L_1}, \hat{f}_i|_{L_1}$ are all $\delta$-close to RS$L_1, \rho$, respectively. Otherwise, $f_0|_{L_0}$ and $f_1|_{L_0}$ are both close to some RS$L_0, \rho$ by the linearity of RS code, respectively. Therefore, by Lemma C.1, for random $\alpha_i$ and codeword $\hat{h}_i|_{L_1} \in RS(L, \rho)$, with probability $1 - |\text{back}(B)|/|\text{back}(L)|$, $\Delta(g_i + \alpha_i h_i + \alpha_i^2 f_i|_{L_1}, \hat{h}_i|_{L_1}) \geq \delta$. Thus, by Lemma C.3,

$$\Pr(\epsilon_i(A_i) \geq \delta) \geq 1 - |\text{back}(B)|/|\text{back}(L)|$$

Next, we prove that in the case mentioned above, it holds

$$\Pr(\epsilon_i(A_i) \geq \delta) \geq 1 - |\text{back}(B)|/|\text{back}(L)|$$

Note that if Inequalities (5) and (6) hold, Inequality (4) will hold. Below are two cases underlying Inequality (6).

On one hand, if there does not exist $B' \subseteq L_1$ and $|B'|/|L_1 + 1| \geq 1 - \delta$, such that $\hat{f}_i(B') = \hat{f}_i(B')$ is some RS codeword, respectively. By Lemma C.1, with probability $1 - |\text{back}(B)|/|\text{back}(L)|$, the relative Hamming distance between $\hat{h}_i + \alpha_i h_i + \alpha_i^2 f_i|_{L_1}$ and $\hat{h}_i + \alpha_i h_i + \alpha_i^2 f_i|_{L_1}$ is greater than $\delta$. Then by Lemma C.3, $\epsilon_i(A_i) \geq \delta$.

On the other hand, there exists such $B' \subseteq L_1$ and $|B'|/|L_1 + 1| \geq 1 - \delta$. Set $\hat{f}_i(B') = \hat{f}_i(B')$, and suppose the following relation holds if $x \in B'$:

$$\hat{g}_i(x) = \hat{h}_i(x), \hat{f}_i(x) = \hat{h}_i(x)$$

By properties of random linear combination, with probability at least $1 - |\text{back}(B')|/|L_1|$, the relative Hamming distance between $f_i(x)$ and $\hat{f}_i(x)$ is not less than the Hamming distance between $\hat{f}_i(x)$ and $f_i(x)$. Therefore, below we only need to consider the following case:

$$\hat{h}_i(x) \geq \hat{h}_i(x), \hat{f}_i(x) = \hat{h}_i(x)$$

In this case, for $x \in D_1 \setminus B'$, $\hat{h}_i(x) = \hat{h}_i(x)$, $\hat{g}_i(x) = \hat{g}_i(x)$, $\hat{f}_i(x) = \hat{f}_i(x)$, and $\hat{h}_i(x)$ is the number of points in $B'$ which is not less than the Hamming distance between $\hat{f}_i(x)$ and $f_i(x)$.

Therefore, we only need to prove Inequality (4) in the following case: (a) For all $i \geq 1$, $\Delta(f_i(x), RS(L, \rho)) \leq \delta$; (b) For all $i \geq 2$, $\Delta(\hat{f}_i(x), RS(L, \rho)) \leq \delta$; (c) At least one of $\Delta(f_i(x), RS(L, \rho)) \geq \delta$ and $\Delta(\hat{f}_i(B), RS(L, \rho)) \geq \delta$ holds.
Since \[ \frac{\text{back}_{i+1}(C \setminus B')}{D} = \frac{|C \setminus B'|}{|D|_{i+1}} = \frac{|C|}{|D|_{i+1}} - \frac{|B|}{|D|_{i+1}}, \] we have
\[ |\text{back}_{i+1}(C) \cap \text{err}_{i+1}| - \frac{|C|}{|D|_{i+1}} \geq |\text{back}_{i}(B) \cap \text{err}_{i}| - \frac{|B|}{|D|_{i}}. \]
So \( \varepsilon_{i+1}(C) \geq \varepsilon_{i}(B) \). Inequalities (6) and (4) hold.

D Proof of Theorem 3.2

**Proof.** Completeness and polynomial binding. Polynomial binding directly comes from HyperPlonk. The main differences between PC_m and HyperPlonk lie in the usage of rolling batch FRI and random polynomial \( r \). The completeness of PC_m follows from that of HyperPlonk and rolling batch FRI.

**Soundness.** We bound the soundness error via two cases.

- **Case 1.** There exists some polynomial \( \hat{f}_i \) for \( i \in [0, \mu - 1] \), which has a degree at least \( 2^{r-i} \). According to Theorem 3.1, the verification passes with a probability bounded by \( \varepsilon_{\text{FRI}} \).

- **Case 2.** For every \( i \in [0, \mu - 1] \), the degree of \( \hat{f}_i \) is less than \( 2^{r-i} \). Suppose that \( \hat{f}(x) \neq y \). We have \( \hat{f}(x) + \alpha \cdot \tilde{r}(x) = y + \alpha \cdot y \) holds with a probability bounded by \( 1/|\mathbb{F}| \) due to the randomness of \( \alpha \). Otherwise, there must exist some \( i \) such that \( \hat{f}(X^i) \neq \tilde{g}_{i-1}(X) + x_i \cdot \tilde{h}_{i-1}(X) \) but for every query, the equation holds. Assume that \( j \) is the smallest of these \( i \)'s. By definition, \( \tilde{g}_{j-1}(X^2) = \hat{f}_{j-1}(X) + \hat{f}_{j-1}(-X) \), and \( \hat{h}_{j-1}(X^2) = 2\hat{f}_{j-1}(X) - \hat{f}_{j-1}(-X) / 2 \). Set \( g(X) \) to be
\[
\hat{f}(X^2) - \frac{\hat{f}_{j-1}(X) + \hat{f}_{j-1}(-X)}{2} - x_j \cdot \frac{\hat{f}_{j-1}(X) - \hat{f}_{j-1}(-X)}{2}.
\]
As \( \hat{f}(X) \neq \hat{g}_{j-1}(X) + x_j \cdot \hat{h}_{j-1}(X) \), \( g \) is a non-zero polynomial of degree less than \( 2^{r-j} \). By the Schwartz–Zippel lemma, the verification passes with a probability of no more than \( (2^{r-j})/|\mathbb{F}| \). By the union bound argument, the total soundness error is less than \( \varepsilon_{\text{FRI}} + (2^{r-j})/|\mathbb{F}| + 1/|\mathbb{F}| \) for \( \varepsilon_{\text{FRI}} \) in Theorem 3.1.

**Knowledge soundness.** Similar to HyperPlonk, knowledge soundness comes from the extractability of Merkle trees and efficient decoding algorithms for RS code. We omit the proof.

2q-bound knowledge leaking. Figure 5 gives the simulator. In Step 3 of Eval_m, a random \( \hat{f} \) can always be found when \( 2q + m \leq 2^{r-1} \). The consistency check in the first round always passes as only evaluations corresponding to \( \{ \pm \beta \}_{i \in [0]} \) would be opened and \( \hat{f}(\pm \beta) = \hat{f}(\pm \beta) \). In addition, \( \{ f_{i} \}_{i \in [n]} \) are valid, so consistency checks in other rounds will pass. Due to random \( r, \hat{f}' \) is uniformly distributed. So, no verifier can notice the simulation with non-negligible probability.

E Proof of Theorem 4.1

**Proof.** Liveness. If the dealer \( P_d \) is honest, then every party will receive their share in the Share phase, so there will be at least \( 2r + 1 \) valid Echo messages sent by honest parties. Also, every honest party will send a Ready message, which means every honest party will complete the Share phase.

**Agreement.** Suppose an honest party \( P_i \) completes the Share phase; we consider the case for every other honest party \( P_j \). We first prove that they will receive \( 2r + 1 \) Ready's. Completion means \( P_i \) must have received \( 2r + 1 \) Ready’s according to Step 14 in Algorithm 3 with at least \( t + 1 \) sent by honest parties. From Step 12, if an honest party who has not sent Ready receives \( t + 1 \) Ready’s, it will send Ready. Thus, every honest party will eventually receive at least \( 2r + 1 \) Ready’s.

Next, we prove every honest party will receive \( t + 1 \) Echo messages. An honest party sends Ready only via Step 10 or Step 12. If all honest parties send Ready by Step 12, there must be \( t + 1 \) Ready’s sent by dishonest parties, which is impossible. Thus, at least one honest party has sent Ready by Step 10. Consequently, at least \( t + 1 \) honest parties have sent the Echo’s. So, \( P_j \) will eventually receive \( t + 1 \) valid Echo’s. It can then obtain its share \( f_j \) and complete the Share phase.

**Correctness.** If the dealer \( P_d \) is honest, then \( f(X, Y) \) only corresponds to a set of the same secret that \( s = f(z, 0) \), so honest parties will reconstruct the same secret. If an honest party \( P_i \) reconstructs \( z_i \), every honest party receives at least \( t + 1 \) valid Echo messages corresponding to a common commitment of a bivariate polynomial, so they reconstruct the same secret.

**Secrecy.** If the dealer \( P_d \) is honest and the corrupted set of \( A \) is \( \{ P_{i} \}_{i \in [\ell - \epsilon]} \), then \( A \) will get univariate polynomials \( \tilde{f}(w_{\lambda}', Y) \) and \( f(X, w_{\lambda}') \) for all \( i \in [\ell - \epsilon] \) along with the proof of these polynomials’ evaluations. According to Theorem 3.2, the evaluation proof only leaks \( \ell \) queried evaluations of \( f \). As the variable degree of \( X \) and \( Y \) are both \( r \), \( A \) has no extra information about polynomial \( \tilde{f}(X, 0) \) and the secret \( s = f(z, 0) \).