

# Multivariate Commitments for a Single Degree Bound

Ryan Lehmkuhl   Alessandro Chiesa

UC Berkeley

This scheme is an extension of [PST13] to support the hiding strategy of Marlin [Chi+20]. This technique requires  $B \cdot \ell + 1$  additional elements (where  $B$  is the hiding bound) in  $\text{ck}$ , when compared to PST. We will refer to this commitment scheme as  $\text{MC}_m$ .

For an  $\ell$ -variate polynomial,  $p$ , denote  $\deg(p)$  as the total degree. Let  $\mathcal{W}_{\ell,D}$  be the set of all multisets of  $\{1, \dots, \ell\}$  with cardinality of any individual element at most  $D$ .

**Setup.** On input a security parameter  $\lambda$  (in unary), the number of variables  $\ell \in \mathbb{N}$ , a hiding bound  $B$ , and a maximum degree bound  $D \in \mathbb{N}$   $\text{MC}_m.\text{Setup}$  samples a key pair  $(\text{ck}, \text{rk})$  as follows. Sample a bilinear group  $\langle \text{group} \rangle \leftarrow \text{SampleGrp}(1^\lambda)$  and parse  $\langle \text{group} \rangle$  as a tuple  $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, G, H, e)$ . Sample random elements  $\beta_1, \dots, \beta_\ell \in \mathbb{F}_q$  and  $\gamma \in \mathbb{F}_q^*$ . Then compute the vector:

$$\Sigma := \begin{pmatrix} \{ (\prod_{i \in W} \beta_i) G \}_{W \in \mathcal{W}_{\ell,D}} \\ \gamma G, \{\gamma \beta_i G, \dots, \gamma \beta_i^B G\}_{i \in [\ell]} \end{pmatrix} \in \mathbb{G}_1^{D^\ell + B\ell + 1}$$

Set  $\text{ck} := (\langle \text{group} \rangle, \Sigma)$  and  $\text{rk} := (D, \langle \text{group} \rangle, \gamma G, \beta_1 H, \dots, \beta_\ell H)$ , and then output the public parameters  $(\text{ck}, \text{rk})$ . These public parameters will support  $\ell$ -variate polynomials over the field  $\mathbb{F}_q$  of degree at most  $D$ .

**Commit.** On input  $\text{ck}$ ,  $\ell$ -variate polynomials  $\mathbf{p} := [p_i]_{i=1}^n$  over  $\mathbb{F}_q$ , and randomness  $\omega := [\omega_i]_{i=1}^n$  over  $\mathbb{F}_q$ .  $\text{MC}_m.\text{Commit}$  outputs commitments  $\mathbf{c} := [c_i]_{i=1}^n$  that are computed as follows. If for any  $p_i \in \mathbf{p}$ ,  $\deg(p_i) > D$ , abort. Else, for each  $i \in [n]$ , if  $\omega_i$  is not  $\perp$  then obtain random polynomial  $\bar{p}_i$  with individual degree  $B$  in each variable from  $\omega_i$ , otherwise set  $\bar{p}_i$  to be a zero polynomial. For each  $i \in [n]$ , output  $c_i := p_i(\beta)G + \gamma \bar{p}_i(\beta)G$ .

**Open.** On input  $\text{ck}$ ,  $\ell$ -variate polynomials  $\mathbf{p} := [p_i]_{i=1}^n$  over  $\mathbb{F}_q$ , evaluation point  $\mathbf{z} \in \mathbb{F}_q^\ell$ , opening challenge  $\xi \in \mathbb{F}_q$ , and randomness  $\omega := [\omega_i]_{i=1}^n$  (the same randomness used for  $\text{MC}_m.\text{Commit}$ ),  $\text{MC}_m.\text{Open}$  outputs an evaluation proof  $\pi$  that is computed as follows. If for any  $p_i \in \mathbf{p}$ ,  $\deg(p_i) > D$ , abort. Else, for each  $i \in [n]$ , if  $\omega_i$  is not  $\perp$  then obtain random polynomial  $\bar{p}_i$  of individual degree  $B$  in each variable from  $\omega_i$ , otherwise set  $\bar{p}_i$  to be a zero polynomial. Then compute the linear combination of polynomials  $p(\mathbf{X}) := \sum_{i=1}^n \xi^i p_i(\mathbf{X})$

and  $\bar{p}(\mathbf{X}) := \sum_{i=1}^n \xi^i \bar{p}_i(\mathbf{X})$ . Compute  $\mathbf{w} := [w_j]_{j=1}^\ell$  and  $\bar{\mathbf{w}} := [\bar{w}_j]_{j=1}^\ell$  satisfying:

$$p(\mathbf{X}) - p(\mathbf{z}) = \sum_{j=1}^\ell (X_j - z_j) w_j(\mathbf{X})$$

$$\bar{p}(\mathbf{X}) - \bar{p}(\mathbf{z}) = \sum_{j=1}^\ell (X_j - z_j) \bar{w}_j(\mathbf{X})$$

Such  $\mathbf{w}$  and  $\bar{\mathbf{w}}$  can always be found efficiently by Lemma 0.4. For  $j \in [\ell]$ , set  $\mathbf{w}_j := w_j(\boldsymbol{\beta})G + \gamma \bar{w}_j(\boldsymbol{\beta})G \in \mathbb{G}_1$  and  $\bar{\mathbf{v}} := \bar{p}(\boldsymbol{\beta}) \in \mathbb{F}_q$ . The evaluation proof is  $\pi := ([\mathbf{w}_j]_{j=1}^\ell, \bar{\mathbf{v}})$

**Check.** On input  $\text{rk}$ , commitments  $\mathbf{c} := [c_i]_{i=1}^n$ , evaluation point  $\mathbf{z} \in \mathbb{F}_q^\ell$ , alleged evaluations  $\mathbf{v} := [v_i]_{i=1}^n$  over  $\mathbb{F}_q$ , evaluation proof  $\pi := ([\mathbf{w}_j]_{j=1}^\ell, \bar{\mathbf{v}})$ , and challenge  $\xi \in \mathbb{F}_q$ ,  $\text{MC}_m.\text{Check}$  proceeds as follows. Compute the linear combination  $C := \sum_{i=1}^n \xi^i c_i$ , then compute the linear combination of evaluations  $v := \sum_{i=1}^n \xi^i v_i$ , and check the evaluation proof via the equality  $e(C - vG - \gamma \bar{\mathbf{v}}G, H) = \prod_{j=1}^\ell e(\mathbf{w}_j, \beta_j H - z_j H)$

**Lemma 0.1.** *The commitment scheme  $\text{MC}_m$  achieves completeness following Definition B.1*

*Proof.* Fix any number of variables  $\ell$ , hiding bound  $B$ , maximum degree bound  $D$  and efficient adversary  $\mathcal{A}$ . Let  $(\text{ck}, \text{rk}) \leftarrow \text{MC}_m.\text{Setup}(1^\lambda, \ell, B, D)$  and  $\langle \text{group} \rangle, \mathbb{F}_q$  be the corresponding algebraic structures given by  $(\text{ck}, \text{rk})$ .

Let  $\mathcal{A}(\text{ck}, \text{rk})$  select  $\ell$ -variate polynomials  $\mathbf{p} := [p_i]_{i=1}^n$  over  $\mathbb{F}_q$ , evaluation point  $\mathbf{z} \in \mathbb{F}_q^\ell$ , and opening challenge  $\xi \in \mathbb{F}_q$ . By assumption, we only consider  $\mathcal{A}$  which choose  $\mathbf{p}$ , s.t.  $\deg(\mathbf{p}) \leq D$ .

Given  $\mathbf{c} \leftarrow \text{MC}_m.\text{Commit}(\text{ck}, \mathbf{p})$  and  $\pi \leftarrow \text{MC}_m.\text{Open}(\text{ck}, \mathbf{p}, \mathbf{z}, \xi)$  we show that for  $\mathbf{v} := \mathbf{p}(\mathbf{z})$ :

$$\text{MC}_m.\text{Check}(\text{rk}, \mathbf{c}, \mathbf{z}, \mathbf{v}, \pi, \xi) = 1$$

We demonstrate this directly:

$$\begin{aligned} e(C - vG - \gamma \bar{\mathbf{v}}G, H) &= e\left(\sum_{i=1}^n \xi^i c_i - \left(\sum_{i=1}^n \xi^i v_i\right)G - \gamma \bar{p}(\mathbf{z})G, H\right) \\ &= e((p(\boldsymbol{\beta}) - p(\mathbf{z}) + \gamma(\bar{p}(\boldsymbol{\beta}) - \bar{p}(\mathbf{z})))G, H) \\ &= e\left(\left(\sum_{j=1}^\ell (\beta_j - z_j) w_j(\boldsymbol{\beta}) + \sum_{j=1}^\ell \gamma (\beta_j - z_j) \bar{w}_j(\boldsymbol{\beta})\right)G, H\right) \\ &= e\left(\left(\sum_{j=1}^\ell (\beta_j - z_j) (w_j(\boldsymbol{\beta}) + \gamma \bar{w}_j(\boldsymbol{\beta}))\right)G, H\right) \\ &= \prod_{j=1}^\ell e((\beta_j - z_j) (w_j(\boldsymbol{\beta}) + \gamma \bar{w}_j(\boldsymbol{\beta}))G, H) \\ &= \prod_{j=1}^\ell e(\mathbf{w}_j, \beta_j H - z_j H) \end{aligned}$$

□

**Lemma 0.2.** *The commitment scheme  $\text{MC}_m$  achieves succinctness following Definition B.3*

*Proof.* For a list of  $n$   $\ell$ -variate polynomials, the scheme  $\text{MC}_m$  requires  $n$   $\mathbb{G}_1$  elements to commit to  $\mathbf{c}$ ,  $\ell+1$   $\mathbb{G}_1$  elements for the evaluation proof, and the time to check this proof of evaluation requires  $\ell + 1$  pairings and one variable-base multi-scalar multiplication of size  $n$ . □

**Theorem 0.3.** *The commitment scheme  $\text{MC}_m$  achieves hiding following Definition B.4*

*Proof.* We describe a polynomial-time simulator  $\mathcal{S}$  such that, for every number of variables  $\ell$ , hiding bound  $B$ , maximum degree  $D$ , and efficient adversary  $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ , the adversary  $\mathcal{A}$  cannot distinguish between the real and ideal world experiments.

$\mathcal{S}$  is defined as follows:

$\mathcal{S}.\text{Setup}(1^\lambda, \ell, B, D)$ :

1. Run  $\text{MC}_z.\text{Setup}(1^\lambda, \ell, B, D)$  and define  $\text{trap} := (\text{ck}, \text{rk}, \beta, \gamma)$
2. Output  $(\text{ck}, \text{rk}, \text{trap})$

$\mathcal{S}.\text{Commit}(\text{trap}, k; \boldsymbol{\omega})$ :

1. Parse  $\boldsymbol{\omega}$  as  $[\omega_i]_{i=1}^n$
2. For  $i = 1, \dots, k$ :
  - (a) Obtain the random polynomial  $\bar{p}_i(\mathbf{X})$  from  $\omega_i$
  - (b) Set  $c_i := \bar{p}_i(\beta)\gamma G$
3. Output  $\mathbf{c} := [c_i]_{i=1}^k$

$\mathcal{S}.\text{Open}(\text{trap}, \mathbf{p}, \mathbf{v}, \mathbf{Q}, \xi; \mathbf{r})$ :

1. Parse  $\mathbf{p} := [p_i]_{i=1}^n$ ,  $\mathbf{v} := [v_i]_{i=1}^n$ , and  $\boldsymbol{\omega} := [\omega_i]_{i=1}^n$
2. Parse query set  $\mathbf{Q}$  as  $T \times \mathbf{z}$  for some  $T \subseteq [n]$  and  $\mathbf{z} \in \mathbb{F}_q^\ell$
3. For  $i \in T$ :
  - (a) Obtain the random polynomial  $\bar{p}_i(\mathbf{X})$  from  $\omega_i$
  - (b) Set  $\tilde{v}_i := \bar{p}_i(\mathbf{z}) - \frac{v_i}{\gamma}$
4. Compute  $\bar{v} := \sum_{i=1}^n \xi^i \tilde{v}_i$ ,  $v := \sum_{i=1}^n \xi^i v_i$ ,  $\bar{p}(\mathbf{X}) = \sum_{i=1}^n \xi^i \bar{p}_i(\mathbf{X})$
5. Compute  $\bar{\mathbf{w}} := [\bar{w}_j]_{j=1}^\ell$  which satisfies  $\bar{p}(\mathbf{X}) - \bar{p}(\mathbf{z}) = \sum_{j=1}^\ell (X_j - z_j) \bar{w}_j(\mathbf{X})$
6. If  $\mathbf{z} \neq \beta$ : compute  $\mathbf{w}_j = \bar{w}_j(\beta)\gamma G$
7. Else  $\mathbf{z} = \beta$ : compute  $\mathbf{w}_j = 0G$
8. Output  $\pi = ([\mathbf{w}_j]_{j=1}^\ell, \bar{v})$

Clearly,  $\mathcal{S}$  is polynomial-time. Associated with each  $p_i$  output by  $\mathcal{A}$  there is an independently and randomly sampled degree  $H$  polynomial  $\bar{p}_i$  defined by  $\omega_i$ . We define a polynomial  $\bar{p}_i'$  such that in the real world,  $\bar{p}_i' := \bar{p}_i$ , whereas in the ideal world  $\bar{p}_i' := \bar{p}_i(\mathbf{X}) - \frac{p_i(\mathbf{X})}{\gamma}$ . Observe that each  $\bar{p}_i'$  is, except with negligible probability, at least degree  $B$  in each variable (we will see why this is necessary later) and independently and randomly distributed. It follows that the two polynomials are identically distributed in both worlds for  $\leq B$  queries.

Furthermore, since  $\mathcal{S}.\text{Setup}$  uses  $\text{MC}_m.\text{Setup}$  to generate  $(\text{ck}, \text{rk})$ , we see that  $(\text{ck}, \text{rk})$  is also identically distributed.

We claim that upon fixing  $(\text{ck}, \text{rk})$  and  $\bar{p}_i', \forall i \in [n]$ , the resulting  $c_i$  are given by a deterministic function in  $p_i(\beta)$  and, after fixing a query point  $\mathbf{z}$ , the evaluation proof  $\pi$  is given by a deterministic function in  $(p(\mathbf{X}), \mathbf{z}, \xi)$ . Since these functions are parametrized by values already shown to be identically distributed in the two worlds, it follows that their outputs will also be identically distributed.

We define  $\text{factor} : \mathbb{F}[X_1, \dots, X_\ell] \rightarrow \mathbb{F}[X_1, \dots, X_\ell]^\ell$  to be the polynomial factorizing algorithm at the point  $\mathbf{z}$  described in Lemma 0.4. Note that this is a linear function. We claim that the following relations hold in both worlds:

$$\begin{aligned} c_i(p_i(\beta)) &:= p_i(\beta)G + \bar{p}_i'(\beta)\gamma G \\ \pi &= ([\mathbf{w}_j]_{j=1}^\ell, \bar{v}) \end{aligned}$$

where

$$\mathbf{w}_j(\mathbf{z}, p_i(\mathbf{X})) = \begin{cases} \text{factor}(p(\mathbf{X}) + \gamma \bar{p}'(\mathbf{X}))_j(\beta)G & \text{if } \mathbf{z} \neq \beta \\ 0G & \text{if } \mathbf{z} = \beta \end{cases}, \quad \bar{v}(\mathbf{z}, \xi) = \sum_{i=1}^n \xi^i \bar{p}_i'(\mathbf{z})$$

Now we show that the above describe the outputs of  $\text{MC}_m$  and  $\mathcal{S}$ .

**Indistinguishability of commitments.** In the real world we have:

$$c_i = p_i(\beta)G + \bar{p}_i(\beta)\gamma G$$

since we have defined  $\bar{p}_i' := \bar{p}_i$ , equivalence follows immediately. In the ideal world, we have that:

$$c_i = \bar{p}_i(\beta)\gamma G$$

here we have defined  $\bar{p}_i'(\mathbf{X}) := \bar{p}_i(\mathbf{X}) - \frac{p(\mathbf{X})}{\gamma}$ . Plugging this in we get that:

$$\begin{aligned} c_i &= p_i(\beta)G + \gamma \bar{p}_i'(\beta)G \\ &= p_i(\beta)G + \gamma(\bar{p}_i(\beta) - \frac{p_i(\beta)}{\gamma})G \\ &= \bar{p}_i(\beta)\gamma G \end{aligned}$$

Which is exactly what  $\mathcal{S}$  outputs. Thus, the commitments are indistinguishable with respect to all adversaries.

**Indistinguishability of evaluation proofs.** In the real world,  $\bar{v} = \sum_{i=1}^n \xi^i \bar{p}_i(\mathbf{z})$  which coincides directly since  $\bar{p}_i' = \bar{p}_i$ . In the ideal world we have that  $\bar{v} = \sum_{i=1}^n \xi^i \tilde{v}_i$  which also follows directly since  $\tilde{v}_i = \bar{p}_i'(\mathbf{z})$ . Thus, the  $\bar{v}$  are indistinguishable to all adversaries.

Finally, we consider each  $[\mathbf{w}_j]_{j=1}^\ell$ . In the real world, we have that:

$$\begin{aligned} \mathbf{w}_j &= \text{factor}(p(\mathbf{X}))_j(\beta)G + \gamma \text{factor}(\bar{p}(\mathbf{X}))_j(\beta)G \\ &= \text{factor}(p(\mathbf{X}) + \gamma \bar{p}(\mathbf{X}))_j(\beta)G \end{aligned}$$

since we have defined  $\bar{p}'_i := \bar{p}_i$ , equivalence follows immediately. In the ideal world, we have that:

$$\mathbf{w}_j := \text{factor}(\gamma\bar{p}(\mathbf{X}))_j(\beta)G$$

here we have defined  $\bar{p}'_i(\mathbf{X}) := \bar{p}_i(\mathbf{X}) - \frac{p(\mathbf{X})}{\gamma}$ . Plugging in we get that:

$$\begin{aligned} \mathbf{w}_j &= \text{factor}(p(\mathbf{X}) + \gamma\bar{p}'(\mathbf{X}))_j(\beta)G \\ &= \text{factor}(p(\mathbf{X}) + \gamma(\bar{p}(\mathbf{X}) - \frac{p(\mathbf{X})}{\gamma}))_j(\beta)G \\ &= \text{factor}(\gamma\bar{p}(\mathbf{X}))_j(\beta)G \end{aligned}$$

Thus, our expression for  $[\mathbf{w}_j]_{j=1}^\ell$  is correct. Note that for any polynomial  $q \in \mathbb{F}_q[X_1, \dots, X_\ell]$ , if  $q$  does not contain the indeterminate  $X_j$ , it will be in the kernel of  $\text{factor}(q)_j$ . It follows that each  $\mathbf{w}_j$  leaks whether  $\bar{p}'$  contains the indeterminate  $X_j$ . Thus, in order for the  $\bar{p}'$  to be indistinguishable, we must require that they have at least degree 1 in each of the  $\ell$  indeterminates. We conclude that no adversary can distinguish between the two worlds.  $\square$

**Lemma 0.4.** *Let  $p(\mathbf{X}) \in \mathbb{F}_q[\mathbf{X}]$  be an  $\ell$ -variate polynomial. Then  $\forall \mathbf{z} \in \mathbb{F}_q^\ell$ , there exists polynomials  $w_i(\mathbf{X})$  such that  $p(\mathbf{X}) - p(\mathbf{z}) = \sum_{i=1}^\ell (X_i - z_i)w_i(\mathbf{X})$ . Furthermore, all the  $w_i$ s can be found with a polynomial-time algorithm.*

*Proof.* We can recover each  $w_i$  with a single polynomial division. Start by dividing  $p(\mathbf{X}) - p(\mathbf{z})$  by  $(X_1 - z_1)$  and define the quotient as  $w_1(\mathbf{X})$ . We have can now express  $p(\mathbf{X}) - p(\mathbf{z}) = (X_1 - z_1)w_1(\mathbf{X}) + r(X_2, \dots, X_\ell)$ . Notably, the remainder of the division is a polynomial in terms of  $X_2, \dots, X_\ell$ . We divide this polynomial by  $(X_2 - z_2)$ , yielding  $w_2(\mathbf{X})$  and a remainder in terms of  $X_3, \dots, X_\ell$ . We continue this until we can express  $p(\mathbf{X}) - p(\mathbf{z}) = \sum_{i=1}^\ell (X_i - z_i)w_i(\mathbf{X}) + r$ . We evaluate the indeterminate  $\mathbf{X}$  at  $\mathbf{z}$ :

$$\begin{aligned} p(\mathbf{z}) - p(\mathbf{z}) &= \sum_{i=1}^\ell (z_i - z_i)w_i(\mathbf{X}) + r \\ 0 &= 0 + r \\ \implies p(\mathbf{X}) - p(\mathbf{z}) &= \sum_{i=1}^\ell (X_i - z_i)w_i(\mathbf{X}) \end{aligned}$$

$\square$

## References

- [Chi+20] A. Chiesa, Y. Hu, M. Maller, P. Mishra, N. Vesely, and N. P. Ward. “Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS”. In: *Advances in Cryptology - EUROCRYPT 2020*. 2020, pp. 738–768.
- [PST13] C. Papamanthou, E. Shi, and R. Tamassia. “Signatures of Correct Computation”. In: *Theory of Cryptography*. 2013, pp. 222–242.