Suppose you have multiple polynomial commitments C_1

… C_k

, under k

different commitment schemes (eg. Kate, FRI, something bulletproof-based, DARK…), and you want to prove that they all commit to the same polynomial P

. We can prove this easily:

Let z = hash(C_1 .... C_k)

, where we interpret z

as an evaluation point at which P

can be evaluated.

Publish openings O_1 ... O_k

, where O_i

is a proof that C_i(z) = a

under the i'th commitment scheme. Verify that a

is the same number in all cases.

Explanation

If any two commitments C_i

and C_j

point to different data, then they would almost certainly evaluate to different values at a randomly selected point (this is because if P_i - P_j

is nonzero, then because P_i

and P_j

have some low degree < D

(eg. D = 2^{15}

), P_i - P_j

can only be zero at \le D

points, which is an insignificant fraction of all possible evaluation points). Hence, if there are successful openings at the same random coordinate that return the same value, this shows that all polynomials must be the same.

Choosing the point z

as a hash of all the commitments ensures that there is no way to manipulate the data or the commitments after you learn z

(this is standard Fiat-Shamir reasoning).