Following is the polynomial commitment scheme between Prover and Verfier. I was looking at the KATE scheme and I noticed it could be done differently and easier. Note that it doesn't require trusted setup, nor attaching additional proof to the result $F(t)$

for a challange t

.

Let me know what you think. Is it useful? Can you break it?

Pairing

The pairing is a map $e: G_1 \times G_2 \rightarrow G_T$

where G_1

and G_2

are additive groups and G_T

is multiplicative group.

Both groups have generators. P

for G_1

and Q

for G_2

. These are publically known.

Pairing e

satisfies:

$e(aP, bQ) = e(P, abQ) = e(abP, Q) = e(P,Q)^{ab}$

$e(P, Q)^{a+b} = e(P, Q)^a \cdot e(P, Q)^b$

Commitment

Prover has a secret polynomial F

.

$F(x) = f_0 + f_1x + ... + f_nx^n$

Firstly Prover generates two random secret numbers a

and b

. They are used to hide coefficients of F

and compose new polynomial K

.

$K(x) = (a + bf_0) + (a+bf_1)x + ... + (a+bf_n)x^n$

Second step is projecting K

on $G2$

. It means multiplying all coefficients by Q

. This creates new polynomial Z

over G_2

.

$$Z(x) = K(x)Q \\ Z(x) = (a + bf_0)Q + (a+bf_1)Qx + ... + (a+bf_n)Qx^n \\ Z(x) = Z_0 + Z_1x + ... + Z_nx^n$$

Final part of the commitment is hiding a

on G_1

and b

on G_2

.

$$M = aP \\ N = bQ$$

The commitment C

to polynomial F

can be send to Verifier.

$$C = (Z, M, N)$$

Challange

Knowing C

, Verifier can ask Prover to calculate $F(t)$

for a given t

.

Prover computes $F(t)$

and sends the result back to the verifier.

Verification

Verifier knows: t

, $F(t)$

and $C = (Z, M, N)$

. To make sure $F(t)$

is correct, the following check needs to be satisfied.

$$p(M, (1+t+..+t^n)Q) \cdot p(F(t)P, N) = p(P, Z(t))$$

Reasoning

Following transforms right-hand side of the verification check to the left-hand side.

$$\begin{align} p(P, Z(t)) & = p(P, K(t)Q) \\ & = p(P, Q)^{K(t)} \\ & = p(P, Q)^{(a + bf_0) + (a+bf_1)t + ... + (a+bf_n)t^n} \\ & = p(P, Q)^{a + bf_0 + at + bf_1t + ... + at^n + bf_nt^n} \\ & = p(P, Q)^{a + at + ... + at^n + bf_0 + bf_1t + ... + + bf_nt^n} \\ & = p(P, Q)^{a + at + ... + at^n} \cdot p(P, Q)^{bf_0 + bf_1t + ... + bf_nt^n} \\ & = p(P, Q)^{a (1 + t + ... + t^n)} \cdot p(P, Q)^{b (f_0 + f_1t + ... + f_nt^n)} \\ & = p(aP, (1+t+..+t^n)Q) \cdot p((f_0 + f_1t + ... + f_nt^n)P, bQ) \\ & = p(M, (1+t+..+t^n)Q) \cdot p(F(t)P, N) \end{align}$$