Theory and Practice of Succinct Zero Knowledge Proofs

Lecture 08:
Polynomial Commitments from Bilinear Groups

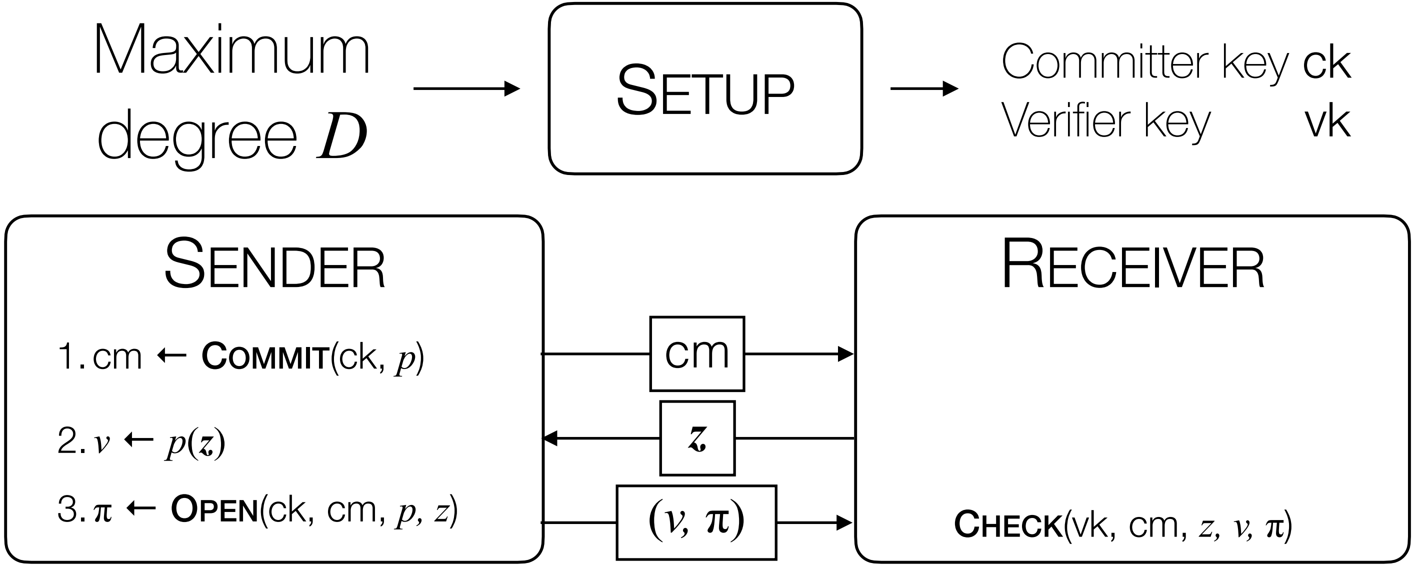
Pratyush Mishra
UPenn
Fall 2023

Announcements

- **First assignment due Wednesday 9/27 midnight (tomorrow!)**
- **First discussion-oriented class 9/28**
- **Project:**
  - List of project ideas is up on Ed.
  - Project proposal **deadline is 10/10**!
  - Talk to me if you're having difficulty choosing a project topic

Polynomial Commitments

Recall: Polynomial Commitments



- **Completeness**: Whenever $p(z) = v$, **R** accepts.
- **Extractability**: Whenever **R** accepts, **S**'s commitment **cm** "contains" a polynomial p of degree at most D.
- **Hiding**: **cm** and **π** reveal *no* information about p other than v

Recall:
Cryptographic Groups

Cyclic Group

A set $\mathbb{G} := \{1, g, g^2, \ldots, g^{p-2}\}$

- g is the generator of $\mathbb{G}$
- p is the *order* of $\mathbb{G}$
- DL: Given an arbitrary $h = g^x$, it is difficult to compute x

Warmup:
Improved Pedersen-based Commitment Scheme

Recall: Pedersen Commitments

$\mathsf{Setup}(n \in \mathbb{N}) \to \mathsf{ck}$

1. Sample random elements $g_1, \ldots, g_n, h \leftarrow \mathbb{G}$

$\mathsf{Commit}(\mathsf{ck}, m \in \mathbb{F}_p^n; r \in \mathbb{F}_p) \to \mathsf{cm}$

1. Output $\mathsf{cm} := g_1^{m_1} g_2^{m_2} \ldots g_n^{m_n} h^r$

Binding: from DL

Hiding: output is uniformly distributed

Additive: given comms to m_1, m_2, can get comm to $\alpha m_1 + \beta m_2$

Recall: PC scheme from Pedersen Comms

$\mathsf{Setup}(d \in \mathbb{N}) \to (\mathsf{ck}, \mathsf{rk})$

1. $\mathsf{ck} \leftarrow \mathsf{Ped}.\mathsf{Setup}(d+1)$. Output $(\mathsf{ck}, \mathsf{rk}) = (\mathsf{ck}, \mathsf{ck})$.

$\mathsf{Commit}(\mathsf{ck}, p \in \mathbb{F}_p^{d+1}; r \in \mathbb{F}_p) \to \mathsf{cm}$

1. Output $\mathsf{cm} := \mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, p; r)$

$\mathsf{Open}(\mathsf{ck}, p, z \in \mathbb{F}_p; r) \to (\pi, v)$

1. Output $(\pi := (p, r), v := p(z))$

$\mathsf{Check}(\mathsf{rk}, \mathsf{cm}, z, v, \pi) \to b \in \{0,1\}$

1. Check $\mathsf{cm} = \mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, p; r)$ and $p(z) = v$.

Better PC scheme from Pedersen Comms?

$\mathsf{Setup}(d \in \mathbb{N}) \to (\mathsf{ck}, \mathsf{rk})$

1. $\mathsf{ck} \leftarrow \mathsf{Ped}.\mathsf{Setup}(d+1)$. Output $(\mathsf{ck}, \mathsf{rk}) = (\mathsf{ck}, \mathsf{ck})$.

$\mathsf{Commit}(\mathsf{ck}, p \in \mathbb{F}_p^{d+1}; r \in \mathbb{F}_p) \to \mathsf{cm}$

1. Output $\mathsf{cm} := \mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, p; r)$

$\mathsf{Open}(\mathsf{ck}, p, z \in \mathbb{F}_p; r) \to (\pi, v)$

1. ???

$\mathsf{Check}(\mathsf{rk}, \mathsf{cm}, z, v, \pi) \to b \in \{0,1\}$

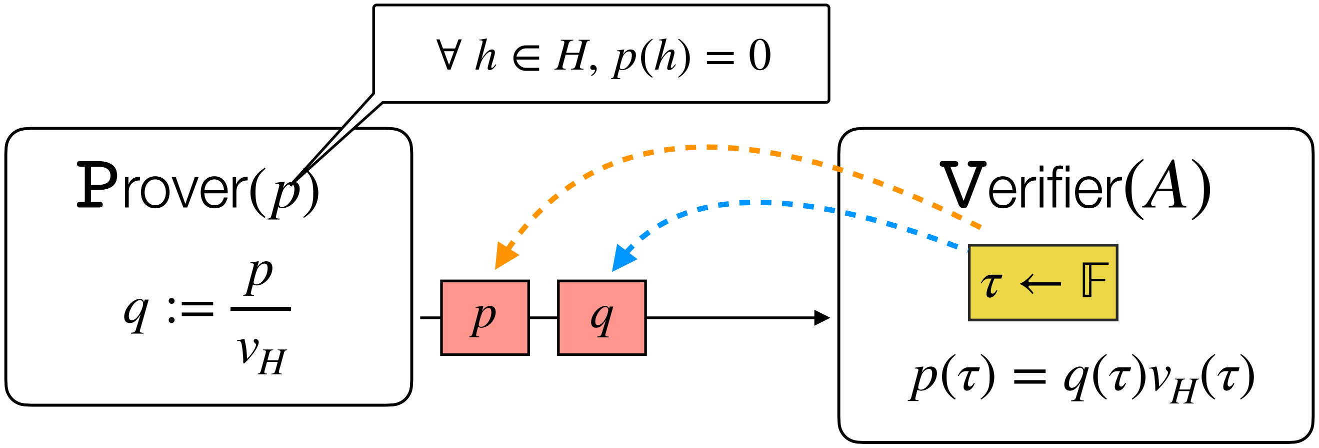
1. ???

Can we use PIOPs to design PC schemes?

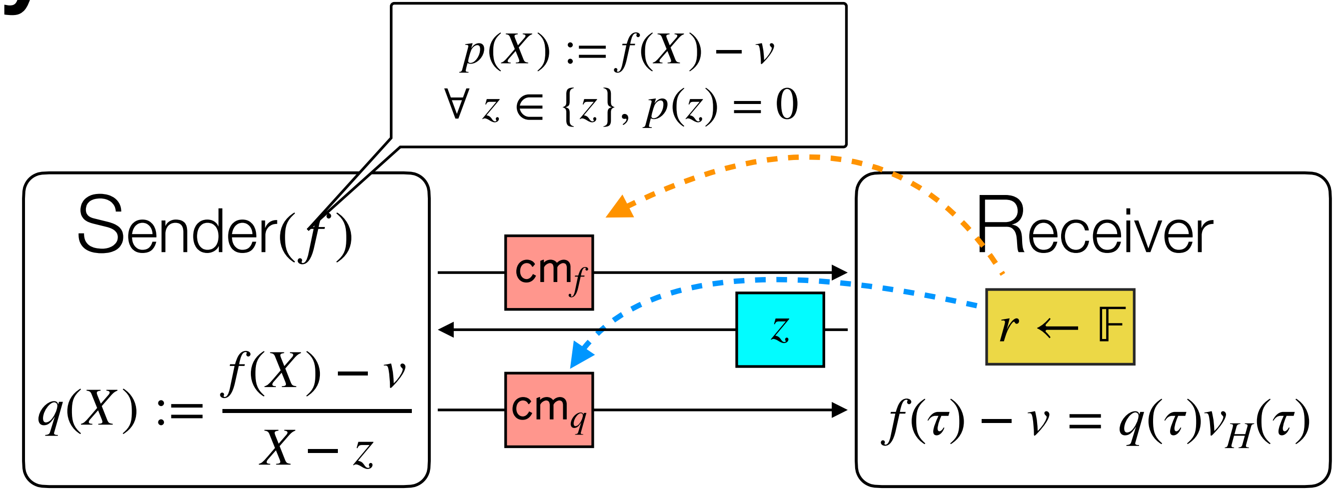
Goal: Want to prove evaluation of $f(X)$ at point z

- We want to show that $f(z) = v$.
    - Equivalently, $f(z) - v = 0$
    - Does this remind you of something?

Recall: ZeroCheck PIOP



Key Idea: Committed ZeroCheck



We set $H := \{z\}$. Vanishing poly $v_H(X) = X - z$.

Are we done?

No! We're actually worse off:
we need to give evaluation proofs for f *and* q!

Idea: What if we hid τ in the exponent?

Warmup 2:
Trusted-Setup
Pedersen-based PC

Trusted Setup Pedersen Commitments

$\mathsf{Setup}(n \in \mathbb{N}) \to \mathsf{ck}$

1. ~~Sample random elements~~ $\cancel{g_0, \ldots, g_n, h \leftarrow \mathbb{G}}$
1. Sample $\tau \leftarrow \mathbb{F}_p$. Output $\mathsf{ck} := (g, g^{\tau}, g^{\tau^2}, \ldots, g^{\tau^{n-1}}, h)$

$\mathsf{Commit}(\mathsf{ck}, m \in \mathbb{F}_p^n; r \in \mathbb{F}_p) \to \mathsf{cm}$

1. Output $\mathsf{cm} := g^{m_1} g^{\tau \cdot m_2} \ldots g^{\tau^{n-1} \cdot m_n} h^r$

Binding: from DL

Hiding: output is uniformly distributed

Additive: given comms to m_1, m_2, can get comm to $\alpha m_1 + \beta m_2$

Trusted Setup Pedersen PC

$\mathsf{Setup}(d \in \mathbb{N}) \to (\mathsf{ck}, \mathsf{rk})$

1. $\mathsf{ck} \leftarrow \mathsf{Ped}.\mathsf{Setup}(d+1)$. Output $(\mathsf{ck}, \mathsf{rk}) = (\mathsf{ck}, \mathsf{ck})$.

$\mathsf{Commit}(\mathsf{ck}, p \in \mathbb{F}_p^{d+1}; r \in \mathbb{F}_p) \to \mathsf{cm}$

1. Output $\mathsf{cm} := \mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, p; r) = g^{p(\tau)}h^r$

$\mathsf{Open}(\mathsf{ck}, p, z \in \mathbb{F}_p; r) \to (\pi, v)$

1. ???

$\mathsf{Check}(\mathsf{rk}, \mathsf{cm}, z, v, \pi) \to b \in \{0,1\}$

1. ???

Key Idea: Committed ZeroCheck

$p(X) := f(X) - v$

$\forall\, z \in \{z\},\ p(z) = 0$

Sender(f)

$$q(X) := \frac{f(X) - v}{X - z}$$

cm_f

z

cm_q

Receiver

1. $\mathsf{cm}_p := \mathsf{cm}_f \cdot \mathsf{Commit}(-z)$
   $= g^{f(\tau)-z}$
2. $\mathsf{cm}_q := g^{q(\tau)}$
3. $\mathsf{cm}_{v_H} := g^{\tau - z}$

We have evaluations at τ in the exponent.

Need to check $f(\tau) - z = q(\tau) \cdot v_H(\tau)$.

How to multiply evaluations and check equality?

Groups allow addition in the exponent

$$g^x \cdot g^y = g^{x+y}$$

How to get multiplication?

We want operation
op such that

$$\mathsf{op}(g^x, g^y) = g^{xy}$$

Unfortunately we don't know of any
such group + operation combinations

Bilinear Groups/
Pairing-friendly Groups

Bilinear groups

- $(p, \mathbb{G}_1, g, \mathbb{G}_T, e)$
  - $\mathbb{G}$ is called the base group
  - $\mathbb{G}_T$ is called the target group
  - These are *different* groups!
  - $\mathbb{G}, \mathbb{G}_T$ are both multiplicative cyclic groups of order p,
  - g is the generator of $\mathbb{G}$.
  - $e(g^x, g^y) : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is called a *pairing*
    - Bilinear: $e(g^x, g^y) = e(g, g^{xy}) = e(g^{xy}, g) = e(g, g)^{xy}$

Kate-Zaverucha-Goldberg Commitment Scheme

KZG Polynomial Commitment

$\mathsf{Setup}(d \in \mathbb{N}) \to (\mathsf{ck}, \mathsf{rk})$

1. $\mathsf{ck} \leftarrow \mathsf{Ped}.\mathsf{Setup}(d+1)$. Output $(\mathsf{ck}, \mathsf{rk}) = (\mathsf{ck}, (g, g^{\tau}))$.

$\mathsf{Commit}(\mathsf{ck}, f \in \mathbb{F}_p^{d+1}) \to \mathsf{cm}$

1. Output $\mathsf{cm} := \mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, f) = g^{f(\tau)}$

$\mathsf{Open}(\mathsf{ck}, f, z \in \mathbb{F}_p) \to (\pi, v)$

1. Output $(\pi, v) := (\mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, q(X) := \dfrac{f(X)}{X - z}) = g^{q(\tau)}$

$\mathsf{Check}(\mathsf{rk}, \mathsf{cm}, z, v, \pi) \to b \in \{0,1\}$

1. ???

KZG Polynomial Commitment

$\mathsf{Setup}(d \in \mathbb{N}) \to (\mathsf{ck}, \mathsf{rk})$

1. $\mathsf{ck} \leftarrow \mathsf{Ped}.\mathsf{Setup}(d+1)$. Output $(\mathsf{ck}, \mathsf{rk}) = (\mathsf{ck}, (g, g^{\tau}))$.

$\mathsf{Commit}(\mathsf{ck}, f \in \mathbb{F}_p^{d+1}) \to \mathsf{cm}$

1. Output $\mathsf{cm} := \mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, f) = g^{f(\tau)}$

$\mathsf{Open}(\mathsf{ck}, f, z \in \mathbb{F}_p) \to (\pi, v)$

1. Output $(\pi, v) := (\mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, q(X) := \dfrac{f(X)}{X - z}) = g^{q(\tau)}$

$\mathsf{Check}(\mathsf{rk}, \mathsf{cm}, z, v, \pi) \to b \in \{0,1\}$

1. Check $e(\mathsf{cm} \cdot g^{-v}, g) \stackrel{?}{=} e(\pi, g^{\tau - z})$

Completeness

$\mathsf{Check}(\mathsf{rk}, \mathsf{cm}, z, v, \pi) \to b \in \{0,1\}$

1. Check $e(\mathsf{cm} \cdot g^{-v}, g) \stackrel{?}{=} e(\pi, g^{\tau - z})$

If Sender is honest, then we can rewrite the check as follows:

$$e(\mathsf{cm} \cdot g^{-v}, g) \stackrel{?}{=} e(\pi, g^{\tau - z})$$

$$e(g^{f(\tau)-v}, g) \stackrel{?}{=} e(g^{q(\tau)}, g^{\tau - z})$$

$$e(g, g)^{f(\tau)-v} \stackrel{?}{=} e(g, g)^{q(\tau)\cdot(\tau - z)}$$

$$e(g, g)^{f(\tau)-v} \stackrel{?}{=} e(g, g)^{\frac{f(\tau) - v}{\tau - z}\cdot(\tau - z)}$$

$$e(g, g)^{f(\tau)-v} \stackrel{?}{=} e(g, g)^{f(\tau)-v}$$

Knowledge Soundness

- **Goal:** We want adv. sender $\mathscr{A}$ to be able to produce a valid proof only if it knows f such that cm_f.
- **Intuition:**
  - Assume $f(z) \neq v$.
  - Then $q(X) = \dfrac{f(X) - v}{X - z}$ is a *rational* function, and not a polynomial.
  - Remember that $\mathbb{G}$ only allows additions in the exponent, not multiplications or divisions (without pairing)
  - So $\mathscr{A}$ can't produce commitment to $q(X)$
- **Formalized** via a proof in the **Generic Group Model**
  - GGM says that whenever $\mathscr{A}$ produces a group element, it must provide an explanation in terms of linear combination of previous group elements.

KZG Demo

“Type-3” Bilinear groups

- $(p, \mathbb{G}_1, g, \mathbb{G}_2, h, \mathbb{G}_T, e)$
  - $\mathbb{G}_1$ and $\mathbb{G}_2$ are called the base groups
  - $\mathbb{G}_T$ is called the target group
  - $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are all multiplicative cyclic groups of order p,
  - g is the generator of $\mathbb{G}_1$, h is the generator of $\mathbb{G}_2$.
  - $e(g^x, h^y) : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is called a *pairing*
    - Bilinear: $e(g^x, h^y) = e(g, h^{xy}) = e(g^{xy}, h) = e(g, h)^{xy}$