Theory and Practice of Succinct Zero Knowledge Proofs

Lecture 07:
Polynomial Commitments from Discrete Logarithms

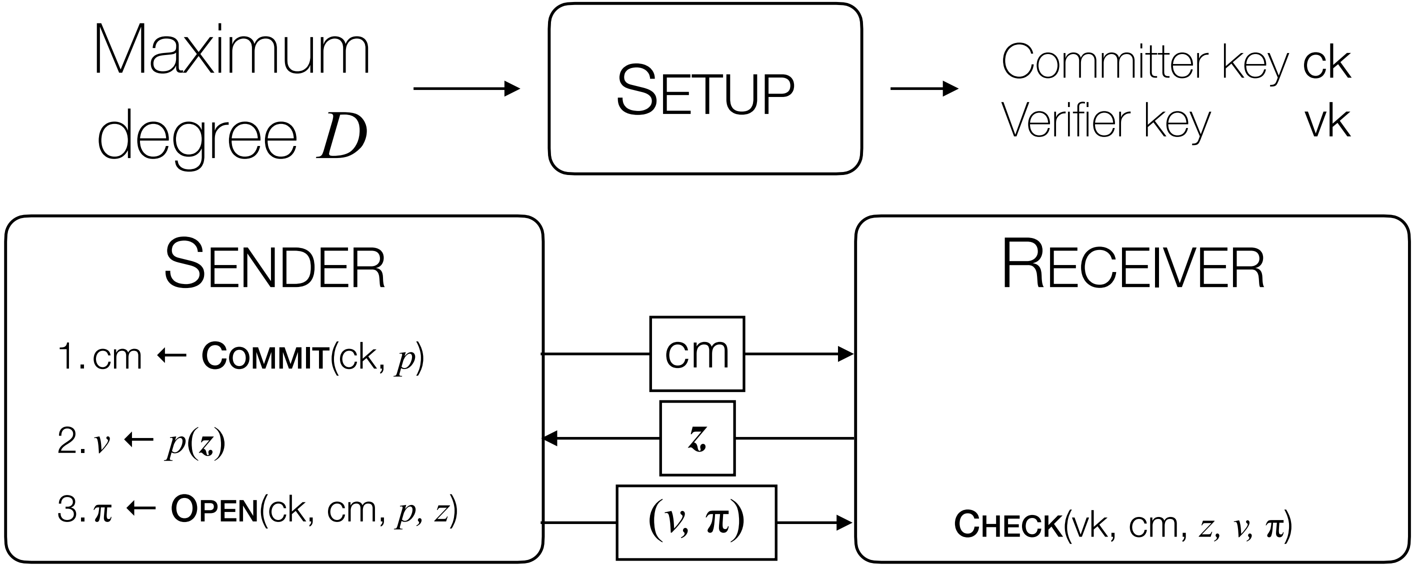
Pratyush Mishra
UPenn
Fall 2023

Announcements

- **Project:**
    - List of project ideas is up on Ed.
    - Project proposal **deadline is 10/10**!
- **Presentations:**
    - First discussion-oriented class **next week, 09/28**.
    - Will put discussion questions on Canvas over the weekend.

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

Cryptographic Groups

Group

A set $\mathbb{G}$ and an operation *

1. Closure: For all $a, b \in \mathbb{G}$, $a * b \in \mathbb{G}$
2. Associativity: For all $a, b, c \in \mathbb{G}$, $(a * b) * c = a * (b * c)$
3. Identity: There exists a unique element $e \in \mathbb{G}$ s.t. for every $a \in \mathbb{G}$, $e * a = a * e = a$.
4. Inverse: For each $a \in \mathbb{G}$, there exists $b \in \mathbb{G}$ s.t. $a * b = b * a = e$

E.g.: integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ under +

positive integers mod prime $p : \{1, 2, \ldots, p-1\}$ under ×

elliptic curves

Generator of a group

- An element g that generates all elements in the group by taking all powers of g

Examples: $\mathbb{F}_7^* := \{1,2,3,4,5,6\}$

$$3^1 = 3; \quad 3^2 = 2; \quad 3^3 = 6$$
$$3^4 = 4; \quad 3^5 = 5; \quad 3^6 = 1 \qquad \text{mod } 7$$

Discrete logarithm assumption

- A group $\mathbb{G}$ has an alternative representation as the powers of the generator $g: \{g, \ g^2, \ g^3 \ , \ldots, \ g^{p-1}\}$
- Discrete logarithm problem:

  given $y \in \mathbb{G}, \quad \text{find } x \quad \text{s.t.} \quad g^x = y$
- Example: Find x such that $3^x = 4 \bmod 7$

- Discrete-log assumption: discrete-log problem is computationally hard

Prime-order groups

- We will use only *prime-order groups*,
  i.e. groups where $|\mathbb{G}|$ is a large prime.
- Main examples of such groups are elliptic curve groups.
- We will call the field $\mathbb{F}_p$ the *scalar field* of the group.

Pedersen Commitment Scheme

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

Goal: For all efficient adv. $\mathscr{A}$,

$$\Pr\left[\mathsf{Commit}(m;r) = \mathsf{Commit}(m';r') \ : \ \begin{array}{c} \mathsf{ck} \leftarrow \mathsf{Setup}(n) \\ (m,r,m',r') \leftarrow \mathscr{A}(\mathsf{ck}) \end{array}\right] \approx 0$$

Proof: We will reduce to hardness of DL. Assume that $\mathscr{A}$ did indeed find breaking (m,r,m',r'). Let's construct $\mathscr{B}$ that breaks DL. Assume that $n = 1$.

Key idea: Let $h = g^x$. Then

$$g^m h^r = g^{m'} h^{r'} \implies g^{m+xr} = g^{m'+xr'}$$

Can recover $x = \dfrac{m - m'}{r' - r}$

$\mathscr{B}(g,h)$

1. $(m,r,m',r') \leftarrow \mathscr{A}(\mathsf{ck} = (g,h))$
2. Output $x = \dfrac{m-m'}{r'-r}$

Hiding

Goal: For all m, m', and all adv. $\mathscr{A}$,
$\mathscr{A}(\mathsf{Commit}(m; r)) = \mathscr{A}(\mathsf{Commit}(m'; r'))$

Proof idea: Basically one-time pad!
Let $\mathsf{cm} := \mathsf{Commit}(\mathsf{ck}, m; r)$. Let $h = g^x$.
Then, for any m', there exists r' such that $\mathsf{cm} := \mathsf{Commit}(\mathsf{ck}, m'; r')$.

We could compute it, if we knew x: $r' = \dfrac{m - m'}{x} + r$

[Note: this doesn't break binding, because $\mathscr{A}$ doesn't know x

Additive Homomorphism

Let cm and cm' be commitments to m and m' wrt r and r'.

Then $\mathsf{cm} + \mathsf{cm}'$ is a commitment to $m + m'$ wrt $r + r'$

$$\mathsf{cm} := g_1^{m_1} \ldots g_n^{m_n} h^r + \mathsf{cm}' := g_1^{m_1'} \ldots g_n^{m_n'} h^{r'}$$

$$= g_1^{m_1 + m_1'} \ldots g_n^{m_n + m_n'} h^{r + r'}$$

$$= \mathsf{Commit}(\mathsf{ck}, m + m'; r + r')$$

PC from DL-hard groups

PC scheme from Pedersen Comms

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

1.

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

1.

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

1.

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

1.

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.

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

1.

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

1.

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.

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.

Completeness

Follows from correctness of Pedersen: recomputing the commitment works.

Extractability

Follows from binding of Pedersen.

$\mathcal{E}(\mathsf{ck}, z)$

1. Invoke $\mathsf{cm} \leftarrow \mathcal{A}(\mathsf{ck})$
2. Get $(\pi = (p; r), v) \leftarrow \mathcal{A}(z)$.
3. Output p.

$\mathcal{E}$ outputs incorrect p if and only if $\mathcal{A}$ can provide a different opening for cm

Hiding

Follows from hiding of Pedersen?

cm is perfectly hiding, but $\pi = (p, r)$ reveals polynomial!

Efficiency

cm is succinct (single $\mathbb{G}$ element), but $\pi = (p, r)$ is $O(d)$!

Better PC from DL

PC scheme from [BCGGP16]

Key idea: write polynomial as a $\sqrt{n} \times \sqrt{n}$ matrix, where n is num. coeffs

$$p = \begin{pmatrix} a_1 & \dots & a_m \\ a_{m+1} & \dots & a_{2m} \\ & \vdots & \\ a_{m(m-1)} & \dots & a_{m^2} \end{pmatrix}$$

Q: How to evaluate at z in matrix form?

$$p(z) = (1, z^m, \dots, z^{m(m-1)}) \begin{pmatrix} a_1 & \dots & a_m \\ a_{m+1} & \dots & a_{2m} \\ & \vdots & \\ a_{m(m-1)} & \dots & a_{m^2} \end{pmatrix} \begin{pmatrix} 1 \\ z \\ \vdots \\ z^{m-1} \end{pmatrix}$$

PC scheme from [BCGGP16]

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

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

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

1.

PC scheme from [BCGGP16]

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

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

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

1. Write p as matrix $p = \begin{pmatrix} a_1 & \dots & a_m \\ a_{m+1} & \dots & a_{2m} \\ & \vdots & \\ a_{m(m-1)} & \dots & a_{m^2} \end{pmatrix}$
2. Use Pedersen to commit to rows, obtaining $\mathsf{cm}_1, \dots, \mathsf{cm}_m$
3. Output $\mathsf{cm} := \begin{pmatrix} \mathsf{cm}_1 \\ \vdots \\ \mathsf{cm}_m \end{pmatrix}$

PC scheme from [BCGGP16]

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

1. Recompute $\mathsf{cm} := \begin{pmatrix} \mathsf{cm}_1 \\ \vdots \\ \mathsf{cm}_m \end{pmatrix}$
2. Compute $\vec{z} := (1, z^m, \ldots, z^{m(m-1)})$
3. Compute $\vec{a} = (1, z^m, \ldots, z^{m(m-1)}) \begin{pmatrix} \vec{a}_1 \\ \vdots \\ \vec{a}_m \end{pmatrix}$
4. Output $(\pi := \vec{a}, p(z))$

PC scheme from [BCGGP16]

$\mathsf{Check}(\mathsf{ck}, \mathsf{cm}, z, v, \pi) \to b$

1. Parse $\mathsf{cm} := \begin{pmatrix} \mathsf{cm}_1 \\ \vdots \\ \mathsf{cm}_m \end{pmatrix}$ and $\pi = (\mathsf{pf}, \vec{a})$
2. Compute $\vec{z} := (1, z^m, \ldots, z^{m(m-1)})$
3. Compute $\mathsf{pf} = (1, z^m, \ldots, z^{m(m-1)}) \begin{pmatrix} \mathsf{cm}_1 \\ \vdots \\ \mathsf{cm}_m \end{pmatrix}$
4. Check $\mathsf{pf} = \mathsf{Ped.Commit}(\mathsf{ck}, \vec{a})$
5. Check $v = \langle \vec{a}, (1, z, \ldots, z^{m-1}) \rangle$

Completeness

Follows from homomorphism of Pedersen:

1. If $\mathsf{cm} := \begin{pmatrix} \mathsf{cm}_1 = \mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, \vec{a}_1) \\ \vdots \\ \mathsf{cm}_m = \mathsf{Ped}.\mathsf{Commit}(\mathsf{ck}, \vec{a}_m) \end{pmatrix}$
2. Then $\mathsf{pf} := (1, z^m, \ldots, z^{m(m-1)}) \begin{pmatrix} \mathsf{cm}_1 \\ \vdots \\ \mathsf{cm}_m \end{pmatrix}$ commits to $\vec{a} = (1, z^m, \ldots, z^{m(m-1)}) \begin{pmatrix} \vec{a}_1 \\ \vdots \\ \vec{a}_m \end{pmatrix}$
3. Additionally, by construction, $\vec{a}(z) = v$

Extractability

Follows from binding of Pedersen + rewinding

1. Extractor rewinds $\mathscr{A}$ n times, each time obtaining an evaluation at different points.
2. This gives us n linear equations in n unknowns, which we can solve.
3. Each iteration will be valid unless $\mathscr{A}$ breaks DL

Hiding

Follows from hiding of Pedersen?

cm is perfectly hiding, but $\pi = (\vec{a})$
reveals polynomial (but maybe less info?)

Efficiency

cm is $\sqrt{d}$ $\mathbb{G}$ elements, and π is $\sqrt{d}$ $\mathbb{F}_p$ elements.

Additionally, Check does only $O(\sqrt{d})$ work!