Theory and Practice of Succinct Zero Knowledge Proofs

Lecture 07:
Polynomial Commitments from Discrete Logarithms
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

Maximum degree $D$ → **SETUP** → Committer key $ck$  
Verifier key $vk$

**SENDER**
1. $cm \leftarrow \text{COMMIT}(ck, p)$
2. $v \leftarrow p(z)$
3. $\pi \leftarrow \text{OPEN}(ck, cm, p, z)$

**RECEIVER**
$\text{CHECK}(vk, cm, z, v, \pi)$

- **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 $\pi$ reveal no information about $p$ other than $v$
Cryptographic Groups
A set $\mathbb{G}$ and an operation $\ast$

1. **Closure:** For all $a, b \in \mathbb{G}$, $a \ast b \in \mathbb{G}$

2. **Associativity:** For all $a, b, c \in \mathbb{G}$, $(a \ast b) \ast c = a \ast (b \ast c)$

3. **Identity:** There exists a unique element $e \in \mathbb{G}$ s.t. for every $a \in \mathbb{G}$, $e \ast a = a \ast e = a$.

4. **Inverse:** For each $a \in \mathbb{G}$, there exists $b \in \mathbb{G}$ s.t. $a \ast b = b \ast a = e$

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

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

elliptic curves
Generator of a group

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

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

$$3^1 = 3; \quad 3^2 = 2; \quad 3^3 = 6 \mod 7$$

$$3^4 = 4; \quad 3^5 = 5; \quad 3^6 = 1$$
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 $y \in \mathbb{G}$, find $x$ s.t. $g^x = y$
- Example: Find $x$ such that $3^x = 4 \mod 7$
- 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

Setup\( (n \in \mathbb{N}) \rightarrow \text{ck} \)

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

Commit\( (\text{ck}, m \in \mathbb{F}_p^n; r \in \mathbb{F}_p) \rightarrow \text{cm} \)

1. Output \( \text{cm} := g_1^{m_1}g_2^{m_2} \ldots g_n^{m_n}h^r \)
Binding

Goal: For all efficient adv. $A$,

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

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

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

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

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

1. $(m, r, m', r') \leftarrow A(\text{ck} = (g, h))$  
2. Output $x = \frac{m - m'}{r' - r}$
Hiding

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

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

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

[Note: this doesn’t break binding, because $\mathcal{A}$ doesn’t know $x$]
Additive Homomorphism

Let $\mathbf{cm}$ and $\mathbf{cm}'$ be commitments to $m$ and $m'$ wrt $r$ and $r'$. Then $\mathbf{cm} + \mathbf{cm}'$ is a commitment to $m + m'$ wrt $r + r'$

\[
\mathbf{cm} := g_1^m \ldots g_n^m h^r + \mathbf{cm}' := g_1^{m'} \ldots g_n^{m'} h^{r'} \\
= g_1^{m_1+m'_1} \ldots g_n^{m_n+m'_n} h^{r+r'} \\
= \text{Commit}(\mathbf{ck}, m + m'; r + r')
\]
PC from DL-hard groups
PC scheme from Pedersen Comms

Setup \((d \in \mathbb{N}) \rightarrow (ck, rk)\)
1.

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

Open \(ck, p, z \in \mathbb{F}_p; r \rightarrow (\pi, v)\)
1.

Check \(rk, cm, z, v, \pi \rightarrow b \in \{0,1\}\)
1.
PC scheme from Pedersen Comms

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

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

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

1.

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

1.

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

1.
PC scheme from Pedersen Comms

Setup\((d \in \mathbb{N}) \rightarrow (ck, rk)\)

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

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

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

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

1.

Check\((rk, \text{cm}, z, v, \pi) \rightarrow b \in \{0,1\}\)

1.
PC scheme from Pedersen Comms

Setup\((d \in \mathbb{N}) \rightarrow (ck, rk)\)

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

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

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

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

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

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

1.
Completeness

Follows from correctness of Pedersen: recomputing the commitment works.
Extractability

Follows from binding of Pedersen.

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

\(\mathcal{C}\) outputs incorrect \(p\) if and only if \(\mathcal{A}\) can provide a different opening for \(\text{cm}\)
Hiding

Follows from hiding of Pedersen?

\(cm\) is perfectly hiding, but \(\pi = (p, r)\) reveals polynomial!
cm is succinct (single $\mathbb{G}$ element), but $\pi = (p, r)$ is $O(d)$!
Better PC from DL
PC scheme from [BCGCP16]

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

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

Q: How to evaluate at $z$ in matrix form?

$$p(z) = (1, z^m, \ldots, z^{m(m-1)}) \begin{pmatrix}
a_1 & \ldots & a_m \\
a_{m+1} & \ldots & a_{2m} \\
\vdots & & \vdots \\
a_{m(m-1)} & \ldots & a_{m^2}
\end{pmatrix} \begin{pmatrix}
1 \\
z \\
\vdots \\
z^{m-1}
\end{pmatrix}$$
PC scheme from [BCGCP16]

Setup($d \in \mathbb{N}$) $\rightarrow$ (ck, rk)
1. ck $\leftarrow$ Ped . Setup($\sqrt{d + 1}$). Output (ck, rk) = (ck, ck).

Commit(ck, $p \in \mathbb{F}_p^{d+1}$) $\rightarrow$ cm
1.
PC scheme from [BCGGP16]

**Setup** \(d \in \mathbb{N}\) → (ck, rk)

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

**Commit** \((\text{ck}, p \in \mathbb{F}_p^{d+1}) \rightarrow \text{cm}

1. Write \(p\) as matrix \(p = \begin{pmatrix} a_1 & \ldots & a_m \\ a_{m+1} & \ldots & a_{2m} \\ \vdots \\ a_{m(m-1)} & \ldots & a_{m^2} \end{pmatrix}\)

2. Use Pedersen to commit to rows, obtaining \(\text{cm}_1, \ldots, \text{cm}_m\)

3. Output \(\text{cm} := \begin{pmatrix} \text{cm}_1 \\ \vdots \\ \text{cm}_m \end{pmatrix}\)
PC scheme from [BCGGP16]

Open(ck, p, z ∈ ℤ_p; r) → (π, v)

1. Recompute \( \text{cm} := \begin{pmatrix} \text{cm}_1 \\ \vdots \\ \text{cm}_m \end{pmatrix} \)

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 [BCCGP16]

Check(ck, cm, z, ν, π) → b

1. Parse $\text{cm} := \begin{pmatrix} \text{cm}_1 \\ \vdots \\ \text{cm}_m \end{pmatrix}$ and $\pi = (\text{pf}, \vec{a})$

2. Compute $\vec{z} := (1, z^m, \ldots, z^{m(m-1)})$

3. Compute $\text{pf} = (1, z^m, \ldots, z^{m(m-1)}) \begin{pmatrix} \text{cm}_1 \\ \vdots \\ \text{cm}_m \end{pmatrix}$

4. Check $\text{pf} = \text{Ped}. \text{Commit}(ck, \vec{a})$

5. Check $\nu = \langle \vec{a}, (1, z, \ldots, z^{m-1}) \rangle$
Completeness

Follows from homomorphism of Pedersen:

1. If $\mathbf{cm} := \begin{cases} 
    \mathbf{cm}_1 = \text{Ped} . \text{Commit}(\mathbf{ck}, \vec{a}_1) \\
    \vdots \\
    \mathbf{cm}_m = \text{Ped} . \text{Commit}(\mathbf{ck}, \vec{a}_m) 
\end{cases}

2. Then $\mathbf{pf} := (1, z^m, \ldots, z^{m(m-1)}) \begin{pmatrix} 
    \mathbf{cm}_1 \\
    \vdots \\
    \mathbf{cm}_m 
\end{pmatrix}$ 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, $\vec{a}(z) = \nu$
Follows from binding of Pedersen + rewinding

1. Extractor rewinds $A \ n$ 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 $A$ breaks DL.
Hiding

Follows from hiding of Pedersen?

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

$c_m$ is $\sqrt{d} \ G$ elements, and $\pi$ is $\sqrt{d} \ \mathbb{F}_p$ elements. Additionally, $\text{Check}$ does only $O(\sqrt{d})$ work!