UP TO NOW

- Introduction to the field
- Secure computation protocols
- Interactive zero knowledge from $\Sigma$-protocols
- Pairing-based cryptography
THIS TIME

- Pairing-based NIZK in the CRS model
- An example of Groth-Sahai proofs:
  - efficient NIZK proofs for algebraic relations
BACKGROUND READING


- Alex Escala, Jens Groth. **Fine-Tuning Groth-Sahai Proofs.** PKC 2015
REMINDER: PAIRINGS

❖ **Pairing:** function \( \hat{e}: G_1 \times G_2 \rightarrow G_T \) that satisfies

❖ **Bilinearity:** \( \hat{e}(ag_1, bg_2) = ab \cdot \hat{e}(g_1, g_2) \)

❖ \( \hat{e}([a]_1, [b]_2) = [ab]_T \)

❖ **Non-degenerate:** \( \hat{e}([a]_1, [b]_2) \neq \mathbf{0} \) if \( a, b \neq 0, g_i \neq 0 \)

❖ **Efficiently computable**

❖ **Setup** (\( \kappa \)) returns \( (p, G_1, G_2, G_T, \hat{e}) \)

Basic fact of pairings: \( \hat{e}([a]_1, [b]_2) = \hat{e}([c]_1, [d]_2) \iff ab = cd \)
REMINDER: NIZK
GROTH-SAHAI PROOFS

- Let $\text{Com}$ be a commitment scheme

- **Goal (general):** Given $A_i = \text{Com}(a_i)$, verify that various algebraic equations hold between $a_i$
  
  - $a_i$ can be either a group element ($a_i$) or integer

- **Example goal:**
  
  - for $A_i = \text{Com}(a_i)$, $B_i = \text{Com}(b_i)$, it holds that $C = \text{Com}(\Sigma b_i a_i)$
**GROTH-SAHAII PROOFS**

- Only hardness assumption:
  - The commitment scheme is secure
  - Several instantiations known (XDH, DLIN, ...)

- **Variant 0**: Com is perfectly binding/comp. hiding
  - Perfectly sound/computationally NIZK

- **Variant 1**: Com is comp. binding/perfectly hiding
  - Computationally sound/perfectly NIZK
DUAL-MODE COMMITMENTS

- Use Com with CRS from one of two different distributions
  - \( \text{crs}_0 \) ("binding") or \( \text{crs}_1 \) ("hiding")

Theorem: \( \text{crs}_0 \) and \( \text{crs}_1 \) are indistinguishable

Theorem: \( \text{Com}[\text{crs}_0] \) is perfectly binding

Theorem: \( \text{Com}[\text{crs}_1] \) is perfectly hiding and trapdoor

The only difference is in the CRS. The rest of Com is the same in both cases
DUAL-MODE COMMITMENTS

- Use **Com** with CRS from one of two different distributions
  - **crs₀** ("binding") or **crs₁** ("hiding")

**Theorem:** **crs₀** and **crs₁** are indistinguishable

**Theorem:** **Com[crs₀]** is perfectly binding

**Corollary:** **Com[crs₀]** is computationally hiding

**Theorem:** **Com[crs₁]** is perfectly hiding and trapdoor

**Corollary:** **Com[crs₁]** is computationally binding
**Lemma.** If $\text{crs}_0$ and $\text{crs}_1$ are computationally indistinguishable, and $\text{Com}[\text{crs}_0]$ is perfectly binding, then $\text{Com}[\text{crs}_0]$ is computationally binding.

**Proof:** Assume that $\text{Com}[\text{crs}_0]$ is not comp. binding. Thus, there $\exists$ adv. $A$ that can on input $\text{crs}_0$ produce $(C, m, r, m^*, r^*)$, s.t. $C = \text{Com}(m; r) = \text{Com}(m^*; r^*)$, $m^* \neq m$, with probability $\varepsilon_A$. Assume $\text{Com}[\text{crs}_0]$ is perf. binding. We construct adv. $B$ that distinguishes $\text{crs}_0$ and $\text{crs}_1$ with probability $\varepsilon_B \geq \varepsilon_A / 2 + 1 / 4$.

$B$ is given as an input $\text{crs}_i$ for $i \leftarrow \{0, 1\}$. $B$ sends $\text{crs}_i$ to $A$. If $A$ succeeds, then $B$ outputs $i^* \leftarrow 0$, otherwise $B$ outputs $i^* \leftarrow 1$.

$$
\varepsilon_B = \Pr[i^* = i] = \Pr[i^* = 0 \mid i = 0] \Pr[i = 0] + \Pr[i^* = 1 \mid i = 1] \Pr[i = 1]
= (\Pr[i^* = 0 \mid i = 0] + \Pr[i^* = 1 \mid i = 1]) / 2
= (\Pr[A \text{ succeeds} \mid i = 0] + (1 - \Pr[A \text{ succeeds} \mid i = 1])) / 2
\geq \varepsilon_A / 2 + 1 / 2 - 1 / 4 = \varepsilon_A / 2 + 1 / 4
$$
**GS PROOFS: IDEA**

- Use **Com** with CRS from one of two different distributions
  - \( \text{crs}_0 \) ("binding") or \( \text{crs}_1 \) ("hiding")

GS proofs with Com[crs\(_0\)] are perfectly sound

\( \text{crs}_0 \) and \( \text{crs}_1 \) are indistinguishable

GS proofs with Com[crs\(_1\)] are computationally zero-knowledge

GS proofs with Com[crs\(_0\)] are computationally zero-knowledge

GS proofs with Com[crs\(_1\)] are computationally sound
We need two separate commitment schemes:

- $\text{DMC}_G$, to commit to group elements and
- $\text{DMC}_E$, to commit to exponents

- $\text{DMC}_G$ and $\text{DMC}_E$ have to play well together
- Due to this and DMC requirements, $\text{DMC}_G/\text{DMC}_E$ are somewhat complicated
DIFFERENT INSTANTIATIONS

- Different instantiations of $\text{DMC}_E/\text{DMC}_G$ are known
  - based on say XDH, DLIN, SH assumptions

- We will describe $\text{DMC}_E/\text{GS}$ proof with XDH
  - thus we need to use asymmetric pairings

- Will not have time to describe $\text{DMC}_G$, DLIN/SH setting proofs, ...
DDH: DIFFERENT VIEW

- Denote \( G = (g_1, b) \), \( E = (E_1, E_2) \)
- \( X = (g_1, b, E_1, E_2) \) is a DDH tuple \( \text{iff} \ E = G \) for some scalar \( a \) \( \text{iff} \ E \) and \( G \) are linearly dependent
- **Corollary 1.** \( X = (g_1, b, E_1, E_2) \) is **not** a DDH tuple \( \text{iff} \) \( \{G, E\} \) is a basis of the vector space \( \mathcal{V} = G_1^2 \)
**DDH: DIFFERENT VIEW**

- $X=(g_1, h, E_1, E_2)$ is a DDH tuple if and only if $E = G$ for some scalar $a$ if $E$ and $G$ are linearly dependent.

- **Corollary 2.**
  - $B$ is a DDH tuple $\implies$ each vector $c \in \langle G \rangle$ can be written non-uniquely as $c_1G + c_2E$ while $c \in \langle G \rangle$ cannot be written as $c_1G + c_2E$.
  - $B$ is not a DDH tuple $\implies$ each vector $c \in \mathbb{V}$ can be written uniquely as $c_1G + c_2E$. 
DMCE: IDEA

- We need to create \( \text{crs}_0 \) and \( \text{crs}_1 \) that are computationally indistinguishable under XDH

- **Idea:** let \( \text{crs}_\chi = (g_k, g_1, b, E_1, E_2) \), where each vector \( c \in \mathcal{V} \) can be written uniquely as \( c_1G + c_2E \)

- \( (g_1, b, E_1, E_2) \) is **not** a DDH tuple if \( \chi = 0 \)

- \( (g_1, b, E_1, E_2) \) is a DDH tuple if \( \chi = 1 \)

  each vector \( c \in <G> \) can be written non-uniquely as \( c_1G + c_2E \) while \( c \in <G> \) cannot be written as \( c_1G + c_2E \)
DMC FOR EXPONENTS

1. // $\chi = \text{hiding mode? 1 : 0}$
2. $g_k \leftarrow \text{Setup} (1^\kappa)$
3. $g_1 \leftarrow G_1$, $x, y \leftarrow \mathbb{Z}_p$
4. $G \leftarrow [(1, x)]_1$
5. $E \leftarrow yG + [(0, 1 - \chi)]_1$
6. $\text{crs}_\chi \leftarrow (g_k, G, E)$
7. $t_d \leftarrow y$

$c = \text{Com} (m; r) \leftarrow mE + rG$

$c = \text{Com} (1; 0) = E$

$\chi = 0$: $(g_1, b, E_1, E_2)$ is not a DDH tuple.
$\chi = 1$: $(g_1, b, E_1, E_2)$ is a DDH tuple.
$\text{crs}_0 \approx \text{crs}_1$ due to XDH assumption.

Note: $\text{Com} (1; 0) = E$
PERFECT BINDING WITH CRS₀

- \( \text{crs}_0 = (gk, G = [(1, x)]_1, E \leftarrow yG + [(0, 1)]_1 \)

- \( \text{Com} (m; r) = mE + rG \)

\[
= [(my + r, m + (my + r)x)]_1
\]

\[
= \text{Elgamal} (m; my + r) \quad // \text{r is random}
\]

- Thus \textbf{perfectly binding} and computationally hiding
PERFECT HIDING WITH CRS₁

❖ crs₀ = (gk, \( G = [(1, x)]_1 \), \( E \leftarrow yG \))

❖ Com \((m; r) = mE + rG\)

\[ = (my + r)G \approx \text{random element of } <G> \]

❖ **Perfectly hiding** since \( r \) is random

❖ Since \( \text{crs}_0 \approx \text{crs}_1 \), and DMCE[crs₀] is perfectly binding => this version is computationally binding under XDH
TRAPDOOR WITH CRS$_1$

- $\text{crs}_1 = (gk, G = [(1, x)]_1, E \leftarrow yG)$
- $\text{Com}(m; r) = mE + rG = (my + r)G$
- Set $td \leftarrow y$
- Given $td$ and $m^*$, compute $r^*$ such that $my + r = m^*y + r^*$
- $\text{Com}(m^*; r^*) = (m^*y + r^*)G = (my + r)G = \text{Com}(m; r)$
- Clearly trapdoor
**Theorem.** Assume XDH holds. $\text{DMCE}_E$ is either perfectly binding and computationally hiding (if $\text{crs}_0$ is used), or computationally binding, perfectly hiding, and trapdoor (if $\text{crs}_1$ is used).

**Proof.** Given on previous pages.
FIRST GROTH-SAHAI PROOF

❖ **Goal:**

❖ Given $Z_i = \text{Com}(z_i, r_i) \in G_1^2$ and $A_i, T \in G_2$

❖ Construct NIZK proof that $\sum z_i A_i = T$

❖ Denote $(A, B) \circ C := (A \circ C, B \circ C)$

❖ Bilinear operation!
**Goal:** given $Z_i = \text{Com}(z_i, r_i), A_i, T$, prove that

$$\sum z_i \cdot A_i = 1 \cdot T \quad (\ast)$$

- The basic idea is always similar
  - Use commitments instead of messages, and additions/bilinear operations in different algebraic domain
  - show that if randomness is zero then

$$\sum (\text{Com}(z_i, 0) \cdot A_i) = \text{Com}(1, 0) \cdot T$$

- For any randomness: to prove $(\ast)$, derive $\pi \in \mathbb{G}_2$ from

$$\sum (\text{Com}(z_i, r_i) \cdot A_i) = \text{Com}(1, 0) \cdot T + (\ldots, \ldots) \cdot \pi$$

- order important: asymmetric pairings
- $\pi$ compensates for added randomness
VERIFICATION WITHOUT PRIVACY

❖ First, consider the case without privacy

❖ $Z_i = \text{Com}(z_i; o) = z_iE + oG$

❖ $\sum (\text{Com}(z_i; o) \bullet A_i) = \sum (z_iE \bullet A_i)$

$= E \bullet (\sum z_iA_i) = E \bullet T$

Thus $\sum (\text{Com} (z_i; o) \bullet A_i) = \text{Com} (1; o) \bullet T$
GENERAL CASE WITH RANDOMNESS

Recall:

- \( \text{crs}_\chi = (g_k, G \leftarrow [(i, x)]_1, E \leftarrow yG + [(0, 1 - \chi)]_1 \)

- \( Z_i = \text{Com}(z_i; r_i) = z_iE + r_iG \)

\[ \sum (Z_i \cdot A_i) = \sum ((z_iE + r_iG) \cdot A_i) = \]

\[ E \cdot (\sum z_iA_i) + G \cdot (\sum r_iA_i) = T =: \pi \]
**GS PROOF OF** \[ \sum_i Z_i A_i = T \]

1. \( \chi = \text{[hiding mode]} \)
2. \( g_k \leftarrow \text{Setup}(1^\kappa) \)
3. \( g_1 \leftarrow G_1, x, y \leftarrow \mathbb{Z}_p \)
4. \( G \leftarrow \{(i, x)\}_i \)
5. \( E \leftarrow yG + [(0, 1 - \chi)]_1 \)
6. \( \text{crs}_\chi \leftarrow (g_k, G, E) \)
7. \( \text{td} \leftarrow y \)

---

\[ \text{crs}_\chi, (\{A_i, Z_i\}, T), (\{x_i, r_i\}) \]

\[ \pi \leftarrow \sum r_i A_i \in G_2 \]

Accept if \( \sum (Z_i \cdot A_i) = E \cdot T + G \cdot \pi \)
SOUNDNESS WITH CRS₀

- \( \text{crs}_0 = (g_k, G = [(1, x)], E \leftarrow yG + [(0, 1)]) \)
- Assume \( Z_i = \text{Com} (z_i; r_i) = z_iE + r_iG \) for some \( z_i \)

Component-wise verification:

\[ \Sigma ((z_i E_1 + r_i g_1) \cdot A_i) = E_1 \cdot T + g_1 \cdot \pi \]

\[ \Sigma ((z_i E_2 + r_i h) \cdot A_i) = E_2 \cdot T + h \cdot \pi \cdot x \]

\[ \Sigma ((z_i g_1 + o) \cdot A_i) = g_1 \cdot T + o \]

Thus \( g_1 \cdot \Sigma z_i A_i = g_1 \cdot T \)

Thus \( \Sigma z_i A_i = T \), as needed
ZERO KNOWLEDGE WITH CRS$_1$

- $\text{crs}_1 = (gk, \ G = [(i, x)]_1, \ E \leftarrow yG$
- Trapdoor com.: $\text{Com} (i; \ o) = E = yG = \text{Com} (o; \ y)$
- Simulator writes $Z_i = \text{Com} (z_i^*; \ r_i^*)$ for $z_i^* = o$ and some $r_i^*$
- **Basic idea:** the simulator creates a GS proof that $\sum z_i^* A_i - t^* T = o$, where $t^*$ is an opening of comm. $E$

- Since prover has $z_i^* = z_i, \ t^* = 1$, the prover must be honest
- Simulator, knowing $y$, can take $z_i^* = t^* = o$
**ZERO KNOWLEDGE**

- $\text{crs}_1 = (gk, \mathbf{G} = [(\mathbf{1}, x)]_1, \mathbf{E} \leftarrow y\mathbf{G}$
- $\text{Com} (\mathbf{1}; o) = \mathbf{E} = y\mathbf{G} = \text{Com} (o; y)$
- Simulator writes $\mathbf{Z}_i = \text{Com}(o; r_i^*) = r_i^*\mathbf{G}$
- Simulator creates $\pi^* \leftarrow \Sigma r_i^*\mathbf{A}_i - yT$ // GS proof for $\Sigma o\mathbf{A}_i - oT = o$
- Verification succeeds:
  
  
  \[ \mathbf{G} \bullet \pi^* = G \bullet (\Sigma r_i^*\mathbf{A}_i - yT) \]
  
  \[ = \Sigma (r_i^*G \bullet \mathbf{A}_i) - yG \bullet T \]
  
  \[ = \Sigma (\mathbf{Z}_i \bullet \mathbf{A}_i) - \mathbf{E} \bullet T \]
SIMULATING PROOF OF $\sum Z_i A_i = T$

1. $\chi = \{\text{hiding mode}\}$
2. $g_k \leftarrow \text{Setup}(1^n)$
3. $g_1 \leftarrow G_1, x, y \leftarrow \mathbb{Z}_p$
4. $G \leftarrow [(i, x)]_1$
5. $E \leftarrow yG + [(0, 1 - \chi)]_1$
6. $\text{crs}_\chi \leftarrow (g_k, G, E)$
7. $td \leftarrow y$

\[\pi^* = \Sigma r_i A_i - yT \in G_2\]

Accept if $\Sigma (Z_i \cdot A_i) = E \cdot T + G \cdot \pi^*$
We saw how to do one concrete GS proof

Details are somewhat scary

but the proof is very efficient

**Prover:** $n$ exponentiations

**Verifier:** $2n + 4$ pairings

**CRS:** 4 group elements

**Proof length:** 1 group element

We used additive notation, so $ag$ is exponentiation
SOME OTHER POSSIBLE SETTINGS FOR GS

✧ Prove you have committed to $X_i, Y_i$, s.t.

✧ $\sum_i (A_i \bullet Y_i) + \sum_i \sum_j a_{ij} (X_i \bullet Y_j) = T$

✧ or to $X_i, y_i$ s.t.

✧ $\sum y_i A_i + \sum b_j X_j + \sum_i \sum_j y_i c_{ij} X_j = T$

✧ where all other values are publicly known
COMPARISON WITH $\Sigma$-PROTOCOLS

- **Good:**
  - non-interactive, arguably easier to understand (?)
  - suits well other pairing-based protocols

- **Bad:**
  - often less efficient
  - requires specific algebraic structure
    - pairings, while $\Sigma$-protocols work in many settings

E.g., Groth-Sahai does not work with Paillier
WHY RELEVANT

- Pairing-based primitives are "algebraic"

- **Example.** Boneh-Boyen signature of \( m \) with \( sk_A \)
  
  \[
  s \leftarrow \left[ \frac{1}{1 + (m + sk_A)} \right]_I
  \]

  Verification: accept if \( s \cdot ([m]_2 + [sk_A]_2) = [1]_T \)

- In some protocols, cannot reveal \( s \) before the end of the protocol, but need to prove you know \( s \)

- Need GS proof:
  
  \[
  S = \text{Com}(s; r) \land pk = [sk_A]_2 \land s \cdot ([m]_2 \cdot [sk_A]_2) = [1]_T
  \]
GS PROOF FOR CIRCUITS

- Recall: to show that circuit is correctly computed, one needs a ZK proof that the committed value is Boolean.

- ZK proof that $c = \text{Com}(mg; r)$ and $m \in \{0, 1\}$:
  - Include signatures of $0$ and $1$ (but nothing else) to the CRS.
  - Create a randomized commitment $c_{\text{sign}}$ of $\text{Sign}(mg)$.
  - Construct GS proof that $c_{\text{sign}}$ commits to a signature of $mg$.

Need "structure-preserving signatures"
STUDY OUTCOMES

- Efficient NIZK from pairings
- Dual-mode commitment
- Groth-Sahai proofs
  - Idea
  - One example
THIS WAS THE LAST LECTURE

- This was the last lecture
Goal of cryptographic protocols:

- security against malicious adversary

security = correctness + privacy

General design principles
STUDY OUTCOMES (CONT.)

- Most general principle:
  - design passively secure protocol
  - achieve active security by employing ZK proofs

(In the case MPC, one uses different techniques)
STUDY OUTCOMES: PASSIVE SECURITY

- Employing homomorphic cryptography
  - Elgamal, Paillier
- Recursion (BDD, ...)
- Better comp. efficiency by allowing many rounds
- Glimpse to multi-party computation
- Glimpse to garbled circuits
- Pairing-based cryptography
STUDY OUTCOMES: ACTIVE SECURITY

- $\Sigma$-protocols
  - Basic protocols, composition
  - Getting full 4-round ZK from $\Sigma$-protocols
- Pairing-based NIZK protocols
  - Groth-Sahai
FURTHER DIRECTIONS

- Different basic techniques for passive security:
  - lattice-based cryptography, much more garbled circuits, much more multi-party computation, much more pairings

- ... for active security:
  - cut-and-choose, ZK based on other algebraic techniques

- Many **insanely clever** ideas to improve efficiency

- Other aspects: verification, ...

- Concrete applications: e-voting, auctions, e-cash, ...
THIS COURSE IN FIVE YEARS

- More emphasis on quantum-safe protocols
  - Lattice-based crypto
  - Fancy applications like fully homomorphic crypto
- More on information-theoretic crypto // also quantum-safe
- MPC
- Need many more hours :)
- No course in 2017, in 2018 will have 32 lectures
Your math teacher must’ve died early.

你的算术老师死得早了