But first, heap or ZKP problem from midterm.

\[ \text{Notation } \]
\[ \text{ZK}^E(x,y) : x = a^x, y = a^y, y^2 = x^{a^2} + 7 \] 

\[ \text{Original predicate} \]
\[ \text{derived predicate} \]

\[ \text{introduce ephemeral commitment to } x \in \mathbb{Z} \]

\[ \mathbb{k} \{ (x, y, z, r) : x = a^x, y = a^y, z = a^{z^2} + 1 \} \text{ and } \exists x^2 \in \mathbb{Z} \]

\[ \text{ephemeral commitment to } x^2 \]

\[ \text{proof}(x) \]
\[ k_x \cdot z \]
\[ k_v = k \cdot k_y = k_z \]
\[ k_c = k \cdot k_y \]
\[ r = r \]
\[ C = \mathbb{k}(k) \]
\[ K_c = X \cdot Y \cdot k \cdot k_y \cdot k_x \cdot k_t \]

\[ c \]

\[ s_x = k_x + c \]
\[ s_y = k_y + c \]
\[ s_z = k_z + c \]
\[ s_2 = k_2 + c \]

\[ \text{Correctness (sanity check) just on } 5 \text{ using honest} \]
\[ \text{proof} \]

\[ \text{Y}(X) = K_y \cdot Y \cdot c \]
\[ (g^x) \cdot (g^y) \cdot k_2 + c \]
\[ y(k_y \cdot y) = x(k_2 + c) \]
\[ y^2 = x^3 + 7 \]
\[ s_x = k_x \]
$y = x + c$

$y^2 - x^2 = 3$

$y_{k_1} + y_{k_2} - x_{k_1} + y_{k_2} + c x^3 = y_{k_1} - x_{k_2} + c (y^2 + x^3) = y_{k_1} + y_{k_2} + c (7)$

$\text{Extractor:}$

Run A twice to receive same $c, k$ different $c, k'$

$y_{k_1}, y_{k_1}', s_2, s_2', s_2''$, $c, c'$

$y_{k_1} - y_{k_1}' = (s_2 - s_2') / (c' - c)$

$y_{k_1} y_{k_1}' = y (X) / g$

$y_{k_1} y_{k_1}' = y (X) / g$

$z = (s_2 - s_2') / (c' - c)$

$y_{k_1} y_{k_1}' = y (X) / g$

$z = (s_2 - s_2') / (c' - c)$

We start by extracting $(x, y, z, r)$

All satisfying $z = x^2$

$z = x^2$, and $z = x^2$ imply $z = x^2$

Lattices:

Three equivalent definitions:

$\forall \mathbf{a} \in \Lambda$, $\mathbf{a}$ is a subgroup

- We will use them for
- Cryptography constructions
- and cryptanalysis
- Lots of hard problems like SVP, LWE
- Lots of structure (for ZF proofs, homomorphic)
Def'n 1: \( \Lambda \) is a subgroup of \( \mathbb{Z}^n \) for integers \( n \geq 0 \) under addition.

Ex. Lattices over \( \mathbb{Z}^2 \):

\[
\begin{align*}
\mathbb{Z}_0^2 & \quad | \quad 36 \\
\langle (1,2) \rangle & \quad | \quad \langle 0,1 \rangle \\
\langle 0,0 \rangle & \quad | \\
\end{align*}
\]

This is the definition most closely following our group theory style.

Def'n 2: \( \Lambda(A) \) is the integer span of \( A \) is a \((n \times m)\) matrix.

A set of basis vectors which are \( \Lambda \in \mathbb{Z}^m \) the rows of \( A \):

\[
\Lambda(A) = \left\{ \sum_{i=1}^{m} s_i \mathbf{v}_i \mid \mathbf{v}_i \in \mathbb{Z}^n \quad s_i \in \mathbb{Z} \right\}
\]

\[
= \{ \mathbf{x} \in \mathbb{Z}^n \mid A\mathbf{x} = \mathbf{0} \text{ for some } s \in \mathbb{Z} \}
\]

\[
= \{ \mathbf{x} \in \mathbb{Z}^n \mid A^T \mathbf{x} = \mathbf{0} \}
\]

Def'n 3: \( \Lambda(A) = \left\{ \mathbf{x} \in \mathbb{Z}^n \mid \tilde{A}\mathbf{x} = \mathbf{0} \right\} \) is a dual basis.

Assume \( \tilde{A} \) is linearly independent in columns and rows. So (1) & (2) are equal.

\[
\tilde{A} = A^T (AA^T)^{-1}
\]

\[
(A^T A)^{-1} A^T
\]

Claim (no proof): Def'n 3 is equivalent to Def'n 2.
Claim (no proof): Def'n 3 is equivalent to Def'n 2

Lattice problems:
- Shortest vector problem SVP.
  Given a basis \( \mathbf{A} \in \mathbb{Z}_q^{m \times n} \),
  find the smallest non-zero vector in \( \Lambda(\mathbf{A}) \) with maximum distance
  \[ \| \mathbf{x} \| = \sqrt{\sum (x[i])^2} \]
This is thought to be hard for random matrices \( \mathbf{A} \)

- One form relevant to us:
  Given \( \mathbf{A} \), find some \( \mathbf{x} \in \Lambda(\mathbf{A}) \) s.t.
  \[ \| \mathbf{x} \| \leq \sqrt{n} \]
  This is a ball containing hypercube, \( \varepsilon=1,1/\sqrt{m} \)
  example: \( \mathbf{x} = (0,1,0,0,1,\ldots) \)

- Ajtai hash function.
  Setup: Let \( \mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n} \) \( m > 2n \log_2 q \)
  So this is compressing but we show, hard to find collisions must exist.
  \( \mathbb{E}_\mathbf{A} : \{0,1\}^m \rightarrow \mathbb{Z}_q^{m \times n} \)

Claim: Ajtai is collision resistant if SVP is hard
  If we can find \( \mathbf{x}_1 \neq \mathbf{x}_2 \in \{0,1\}^m \)
  such that \( \mathbf{A} \mathbf{x}_1 = \mathbf{A} \mathbf{x}_2 \)
  \( \mathbb{E}(\mathbf{A}) \)
Such that \( \mathbf{Ax}_i = \mathbf{Ax}_2 \)

then we can solve the \( \|x\|_2 \leq \sqrt{n} \) - SVP on \( \Lambda(\tilde{A}) \)

\( \text{Proof:} \) Suppose \( \Lambda(\tilde{A}) \) outputs a \( \|x\|_2 \leq \sqrt{n} \) \( x_1, x_2 \in \mathbb{R}^n \)

We can construct \( \tilde{A}'(\tilde{A}) \) that finds a non-zero vector to solve SVP.

\( \tilde{A}'(\tilde{A}): \) Compute \( \Lambda(\tilde{A}) \)

\( \tilde{\mathbf{Az}} = 0 \)

\( x_1, x_2 \in \Lambda(\tilde{A}) \)

\( x_1 = (0, 0, 0, \ldots, 1) \in \mathbb{R}^n \)

\( x_2 = (1, 1, \ldots) \in \mathbb{R}^n \)

\( \mathbf{Ax}_1 = \mathbf{Ax}_2 \)

\( \mathbf{Ax}_1 - \mathbf{Ax}_2 = 0 \)

\( \|x_1 - x_2\| \)

So \( \mathbf{z} = x_1 - x_2 \) satisfies \( \|\mathbf{z}\|_2 = \sqrt{n} \) SVP.