Lattices

Thursday, October 31, 2019 10:30 AM

But first: Recap of ZKP problem from midterm.

5.2) Notation

$$ZK\{(x,y) : \overset{(1)}{X = g^x} \ \overset{(2)}{Y = g^y} \ \overset{(3)}{y^2 = x^3 + 7}\}$$

original predicate

$\Downarrow$ in exponent simplify

$$g^{y^2} = g^{x^3} g^7$$

$\Downarrow$

$$Y^y = X^{x^2} g^7$$

desired predicate

introduce ephemeral commitment to $C = g^{x^2} h^r$ $\Downarrow$

$$ZK\{(x,y,z,r) : \overset{(1)}{X = g^x} \ \overset{(2)}{Y = g^y} \ \overset{(3)}{C = g^z h^r}\}$$

will prove $z = x^2$

~~and $x^2 = z$~~ $C = X^x h^r$ (4)

~~$Y^y = X^z g^7$~~

$g^7 = Y^y (X^{-1})^z$ (5)

5.3) Prover(x,y)

$k_x \xleftarrow{\$} \mathbb{Z}_p$

k_y

k_z

k_r

$r \xleftarrow{\$} \mathbb{Z}_p$

$C = g^{(x^2)} h^r$

- $K_x = g^{k_x}$, $K_y = g^{k_y}$
- $K_z = g^{k_z} h^{k_r}$
- $K_{z'} = X^{k_x} h^{k_r}$
- $K_{xy} = Y^{k_y} (X^{-1})^{k_z}$

Verifier(X, Y, C)

C — ephemeral commitment to $g^{x^2} h^r$

$\xrightarrow{K_x, K_y, K_z, K_{z'}, K_{xy}}$

$\xleftarrow{c}$

$s_x = k_x + cx$

$s_y = k_y + cy$

$s_r = k_r + cr$

$s_z = k_z + c(x^2)$

(1) $g^{s_x} = K_x X^c$

(2) $g^{s_y} = K_y Y^c$

(3) $g^{s_z} h^{s_r} = C^c K_z$

(4) $X^{s_x} h^{s_r} = C^c K_z'$

(5) $\boxed{Y^{s_y} (X^{-1})^{s_z} = K_{xy}\, g^{7c}}$

Correctness (Sanity check) just on (5) using honest prover

$$(g^y)^{k_y + cy} (g^{-x})^{(k_z + cz)} \qquad Y^{k_y} (X^{-1})^{k_z} g^{7c}$$

$$= (g^y)^{k_y} (g^{-x})^{k_z} g^{7c}$$

$$g^{y(k_y + cy) - x(k_z + cz)} = g^{yk_y - k_z x + 7c}$$

$y^2 = x^3 + 7$

$y^2 - x^3 = 7$

$y = x + 1$

$y^2 - x^3 = z$

$$g^{y k_y + y^2 c - y k_z + c x^3} = g^{y k_y - k_z x + z c}$$

$$g^{y k_y - x k_z + c\underline{(y^2 + x^3)}} = g^{y(k_y - k_z x + c\underline{(z)})} \checkmark$$

5, 9) Extractor: Run $\mathcal{A}$ twice to receive same c, K two challenges and different c, s

c, c'

$\underline{s_y, s_y'}, \quad s_z, s_z', \ldots$

$$Y^{s_y} (X^{-1})^{s_z} / g^{zc} = K_{XY} = Y^{s_y'} \underline{(X^{-1})^{s_z'}} / g^{zc'}$$

$$Y^{s_y - s_y'} (X^{-1})^{s_z - s_z'} = g^{z(c' - c)}$$

$$\underline{z =} \left(\frac{s_y - s_y'}{c' - c}\right) \quad x = \left(\frac{s_z - s_z'}{c' - c}\right)$$

$$Y^{\left(\frac{s_y - s_y'}{c' - c}\right)} (X^{-1})^{\left(\frac{s_z - s_z'}{c' - c}\right)} = g^{z} \quad (5)$$

Our goal is to extract x, y, and show they satisfy

(1) $g^x = X$ (2) $g^y = Y$

(3) $y^2 = x^3 + z$

We start by extracting

$\Rightarrow (X, Y, \underline{z}, r)$ all satisfying (1), (2), (3), (4), (5)

(3) $c = X^x h^r = g^z h^r$ (4)

(1) $\Rightarrow$ (1) $g^x = X$

(2) $\Rightarrow$ (2) $g^y = Y$

(1), (3), (4) imply $z = X^2$

$z = x^2$, and (1), (5) $\Rightarrow g^z = Y^y (X^{-1})^z \Rightarrow g^z = g^{y^2} g^{-x^3} \Rightarrow$ (3) $x^3 + z = y^2$ in original statement

---

Lattices:

- We will use them for
  - cryptography constructions
  - and cryptanalysis
- Lots of hard problems, like SVP, LWE
  Lots of structure (for ZK proofs, homomorphic enc)

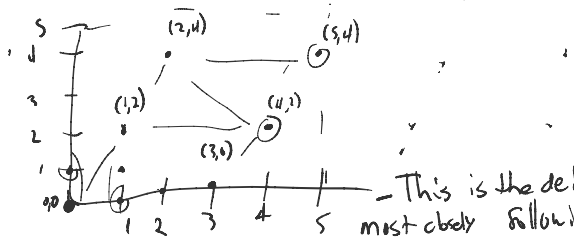
Three equivalent definitions:

Def'n 1: A lattice Λ is a subgroup

Def'n 1: A lattice Λ is a subgroup of $\mathbb{Z}_q^n$ for integers q, n under addition

ex.
Lattices over $\mathbb{Z}_6^2$

$|\mathbb{Z}_6^2| = 36$



$\langle (1,2) \rangle$

$\langle 0,2 \rangle$

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 $A \in \mathbb{Z}_q^{m \times n}$

a set of basis vectors which are the <u>rows</u> of A

$$A^T = \underbrace{\left[(a_1)(a_2)(a_3) \right]}_{m} \Big\} n$$

$$\Lambda(A) = \left\{ \sum_i s_i \cdot a_i \;\middle|\; s \in \mathbb{Z}^m \right\}$$

$$= \left\{ x \in \mathbb{Z}_q^n \;\middle|\; A^T s = x \text{ for some } s \in \mathbb{Z}^m \right\}$$

$n \times 1 \quad \overset{n \times m}{[\quad]^m}$

$\langle g \rangle \qquad \langle g, h \rangle \subseteq G$

$e, g, g^2, \ldots \qquad g^a h^b$ for some $a, b \in \mathbb{Z}^2$

This is the dual form of definition

Def'n 3: $\Lambda(A) = \left\{ x \in \mathbb{Z}_q^n \;\middle|\; \tilde{A} x = 0 \right\}$ $\tilde{A}$ is dual basis of A

Assume A is linearly independent in columns and rows, so ① ② are equal

$$\tilde{A} = \underbrace{A^T (A A^T)^{-1}}_{\text{pseudoinverse}} \quad ①$$

$$(A^T A)^{-1} A^T \quad ②$$

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

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

Lattice problems:

- Shortest vector problem SVP.

  Given a basis $A \in \mathbb{Z}_q^{m \times n}$,

  find the smallest non-zero vector in $\Lambda(A)$ — euclidean distance

  $$\|x\| = \sqrt{\sum_i (x[i])^2}$$

  This is thought to be hard for random matrices A

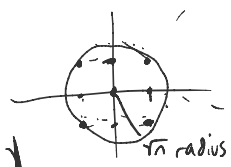
- One form relevant to us:

  Given A, find some $x \in \Lambda(A)$ s.t.

  $$\|x\| \leq \sqrt{n}$$

  This is a ball containing hypercube, $\{-1,0,1\}^n \subset \mathbb{Z}_q^n$

  example: $x = \overbrace{(0,-1,0,0,1,\ldots)}^{n}$



- Ajtai hash function.

Setup: Let $A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$

$m > 2n \log_2 q$

So this is compressing, collisions must exist. But we show hard to find is SVP is hard

Hash: $f_A(x) = Ax$

$f_A : \{0,1\}^m \longrightarrow \mathbb{Z}_q^n$ ← 256 bits

Claim: Ajtai's is collision resistant if SVP is hard

If we can find $x_1 \neq x_2 \in \{0,1\}^m$

such that $Ax_1 = Ax_2$

$\Lambda(\tilde{A})$

Such that $\mathbf{A}x_1 = \mathbf{A}x_2$

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

Proof: Suppose $\mathcal{A}(\mathbf{A})$ outputs a collision $x_1, x_2 \in \{0,1\}^n$

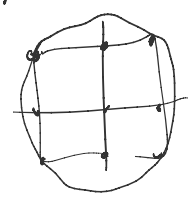
We can construct $\mathcal{A}'(\tilde{A})$ that finds a non-zero vector z, s.t. $\|z\| \le \sqrt{n}$, and $\tilde{A}z = 0$ to solve SVP.

$\mathcal{A}'(\tilde{A})$: compute $\mathbf{A}$ from $\tilde{A}$

$x_1, x_2 \leftarrow \mathcal{A}(\mathbf{A})$

$x_1 = (0, 1, 0 0 0, 1) \in \{0,1\}^n$

$x_2 = (1, 1 \cdots) \in \{0,1\}^n$



$x_1 - x_2$ lies in this hypercube of size 1

$\mathbf{A}x_1 = \mathbf{A}x_2$

$\mathbf{A}(x_1 - x_2) = 0$

and $\|x_1 - x_2\|$

So $z = x_1 - x_2$ satisfies $\|\ \|_2$ SVP