Setup(1^λ): Define lattice parameters $n = n(\lambda)$, $q = q(\lambda)$, $m = \Theta(n \log q)$, $\chi = \chi(\lambda)$, $\sigma = \sigma(\lambda)$

χ: error distribution

σ: width parameter for preimage sampling (will set based on security proof – $s \sim m^{O(d)}$)

Sample $(A, T) \leftarrow \mathsf{TrapGen}(n, q)$ $\quad A \in \mathbb{Z}_q^{n \times m}$

$B_1, \ldots, B_\ell \xleftarrow{R} \mathbb{Z}_q^{n \times t}$ $\quad t = \lceil n \log q \rceil$

$p \xleftarrow{R} \mathbb{Z}_q^n$

Output $\mathsf{mpk} = (A, B_1, \ldots, B_\ell, p)$

$\mathsf{msk} = T$

KeyGen$(\mathsf{mpk}, \mathsf{msk}, f)$: $B_f \leftarrow [B_1 | \cdots | B_\ell] \cdot H_f$ (input-independent evaluation)

$z \leftarrow \mathsf{SamplePre}\left([A | B_f], \begin{bmatrix} T \\ 0 \end{bmatrix}, p, \sigma\right)$

$\begin{bmatrix} T \\ 0 \end{bmatrix}$ is a trapdoor for $[A | B_f]$

output $sk_f \leftarrow z$

Encrypt(mpk, x, μ): Sample $s \xleftarrow{R} \mathbb{Z}_q^n$

Sample $e_1 \leftarrow \chi^m$, $e' \leftarrow \chi$, $R_1, \ldots, R_\ell \leftarrow \{0,1\}^{m \times t}$, $e_2 \leftarrow e_1^T [R_1 | \cdots | R_\ell]$

Output $ct = \left(s^T A + e_1^T,\ s^T [B_1 - x_1 G | \cdots | B_\ell - x_\ell G] + e_2^T,\ s^T p + e' + \mu \cdot \lfloor \tfrac{q}{2} \rceil,\ x\right)$

Decrypt(sk_f, ct): compute $ct_3 - [ct_1 | ct_2 H_{f,x}] z$ and round

Correctness. Suppose $f(x) = 0$. Then

$$\left(s^T [B_1 - x_1 G | \cdots | B_\ell - x_\ell \cdot G] + e_2^T\right) H_{f,x} = s^T (B_f - f(x) \cdot G) + e_2^T H_{f,x} = s^T B_f + e_2^T H_{f,x}$$

Next:
$$\left(s^T [A | B_f] + [e_1^T | e_2^T H_{f,x}]\right) z = s^T t + [e_1^T | e_2^T H_{f,x}] z$$

Thus, we compute

$$\mu \cdot \lfloor \tfrac{q}{2} \rceil + \underbrace{e' - [e_1^T | e_2^T H_{f,x}] z}$$

"small" since e_1, e_2, e' are from noise distribution and $\|H_{f,x}\| \le (n \log q)^{O(d)}$ where d is the depth of the computation

Security. Proving security is delicate. Need to be able to simulate decryption keys, but we do not have a trapdoor for A (otherwise LWE is easy).

- ↳ In other words, if x is the challenge attribute, we need to be able to give out keys for all functions f where $f(x) = 1$ but be unable to give out keys for $f(x) = 0$.
- ↳ Key technique: "punctured trapdoor" that works only for functions f where $f(x) = 1$.

To leverage this technique, we will consider selective security where adversary has to declare attribute before seeing public parameters

Open problem: Adaptively-secure ABE from polynomial hardness of LWE

<u>Proof of Security.</u> We will use a hybrid argument.

<u>Hyb_0</u>: real security game encrypting μ_0

<u>Hyb_1</u>: after adversary selects the challenge attribute $x^* \in \{0,1\}^\ell$, challenger constructs the public key as follows: $(A, T) \leftarrow \mathsf{TrapGen}(n, q)$

$$R_1, \dots, R_\ell \xleftarrow{R} \{0,1\}^{m \times t}$$

$$B_1 \leftarrow AR_1 + x_1^* G, \dots, B_\ell \leftarrow AR_\ell + x_\ell^* G$$

$$\mathsf{mpk} = (A, B_1, \dots, B_\ell, p) \quad \text{where } p \xleftarrow{R} \mathbb{Z}_q^n$$

to answer key-generation queries for f, challenger computes

$$B_f \leftarrow [B_1 | \cdots | B_\ell] \cdot H_f$$

$$z_f \leftarrow \mathsf{SamplePre}\left([A \,|\, B_f], \begin{bmatrix} T \\ 0 \end{bmatrix}, p, s\right)$$

to construct the challenge ciphertext, challenger samples $s \xleftarrow{R} \mathbb{Z}_q^n$, $e_1 \leftarrow \chi^m$, $e' \leftarrow \chi$, $e_2^T \leftarrow e_1^T [R_1 | \cdots | R_\ell]$ and outputs $\mathsf{ct} = (s^T A + e_1^T,\ s^T [B_1 - x_1^* G \,|\, \cdots \,|\, B_\ell - x_\ell^* G] + e_2^T,\ s^T p + e' + \mu \cdot \lfloor \frac{q}{2} \rceil,\ x)$

Hyb_0 and Hyb_1 are statistically indistinguishable by LHL [need a variant where $(A, AR, e^T R) \overset{s}{\approx} (A, \mathcal{U}, e^T R)$]

$e^T R$ is partial leakage on R

(statement holds for all e when $m > 2n \log q$)

<u>Hyb_2</u>: key-generation queries are answered <u>without</u> using trapdoor for A: instead, challenger computes $R_{f,x^*} = [R_1 | \cdots | R_\ell] \cdot H_{f,x^*}$ and outputs

$$z_f \leftarrow \mathsf{SamplePre}\left([A \,|\, B_f], \begin{bmatrix} -R_{f,x^*} \\ I \end{bmatrix}, t, s\right)$$

Hyb_1 and Hyb_2 are statistically indistinguishable by pre-image sampling (when $s \sim m^{O(d)}$). To see this, it suffices to show that $\begin{bmatrix} -R_{f,x^*} \\ I \end{bmatrix}$ is a "short" trapdoor for $[A \,|\, B_f]$. By homomorphic evaluation,

$$[B_1 - x_1^* G \,|\, \cdots \,|\, B_\ell - x_\ell^* G] \cdot H_{f,x} = B_f - f(x^*) \cdot G$$

Now, adversary can only query for keys on function f where $f(x^*) = 1$ (cannot decrypt).

Now:

$$[B_1 - x_1^* G \,|\, \cdots \,|\, B_\ell - x_\ell^* G]\, H_{f,x} = A [R_1 | \cdots | R_\ell] H_{f,x^*} = AR_{f,x^*}$$

Thus,

$$AR_{f,x^*} = B_f - G \implies [A \,|\, B_f] \cdot \begin{bmatrix} -R_{f,x^*} \\ I \end{bmatrix} = -AR_{f,x^*} + B_f = G$$

Moreover $\|R_{f,x^*}\| \le m^{O(d)}$ so the claim holds.

<u>Key observation</u>: Trapdoor <u>only</u> works if $f(x^*) = 1$. If $f(x^*) = 0$, then $AR_{f,x^*} = B_f$ and we do <u>not</u> have a trapdoor for $[A \,|\, B_f]$. Referred to as a "punctured" trapdoor.

<u>Hyb_3</u>: replace challenge ciphertext with $(z_1^T,\ z_1^T [R_1 | \cdots | R_\ell],\ z')$ where $z_1 \xleftarrow{R} \mathbb{Z}_q^m$, $z' \xleftarrow{R} \mathbb{Z}_q$

Hyb_2 and Hyb_3 are indistinguishable under LWE. To see this, let $([A \,|\, p], [z_1^T \,|\, z'])$ be the LWE challenge. We can set the public key as in $\mathsf{Hyb}_2 / \mathsf{Hyb}_3$:

$$R_1, \dots, R_\ell \xleftarrow{R} \{0,1\}^{m \times t}, \quad B_i \leftarrow AR_i + x_i^* \cdot G$$

Simulate secret key queries using procedure in Hyb_2 (only depends on $A, R_1, \dots, R_\ell, t, f, x^*$).

To simulate challenge ciphertext, we output

$$(z_1^T,\ z_1^T [R_1 | \cdots | R_\ell],\ z' + \mu_0 \cdot \lfloor \tfrac{q}{2} \rceil)$$

Suppose $z_1^T = s^T A + e_1^T$ and $z' = s^T p + e'$. Then recall: $B_i = AR_i + x_i^* G$

so $AR_i = B_i - x_i^* G$

$$z_1^T = s^T A + e_1^T$$

$$z_1^T [R_1 | \cdots | R_\ell] = [s^T AR_1 + e_1^T R_1 \ | \cdots | \ s^T AR_\ell + e_1^T R_\ell]$$

$$= s^T [B_1 - x_1^* G \ | \cdots | \ B_\ell - x_\ell^* G] + e_1^T [R_1 | \cdots | R_\ell]$$

$$z' + \mu_0 \cdot \lfloor \tfrac{q}{2} \rceil = s^T p + e' + \mu_0 \cdot \lfloor \tfrac{q}{2} \rceil$$

This is the distribution in Hyb_2.

Alternatively if z_1 and z_2 are uniform, then we have the distribution in Hyb_3.

Claim now follows by hybrid argument: Hyb_3 is independent of μ_0. Can apply same transitions in reverse to encrypt μ_1.

<u>Key idea</u>: Program x^* into the public key.
This yields a trapdoor for $[A | B_f]$ whenever $f(x^*) = 1$.
And ensures semantic security whenever $f(x^*) = 0$.

<u>Predicate encryption</u>: Want ciphertexts to additionally <u>hide</u> the attribute
- Weak attribute hiding: successful decryption also recovers attribute
- Strong attribute hiding: attribute remains hidden even if decryption succeeds
  - ↳ implies functional encryption!

We will focus on the setting of <u>weak</u> attribute-hiding.

<u>Key idea</u>: Combine FHE with ABE. We will encrypt the attribute under ABE and homomorphically evaluate the predicate.
<u>Challenge</u>: How to decrypt the output of the predicate? We will use a "dual-use" technique where the underlying schemes share a <u>common</u> secret key.

First, we will generalize our homomorphic evaluation relations to support <u>matrix-valued</u> computations
- So far: for a function $f : \{0,1\}^\ell \to \{0,1\}$:
$$[B_1 | \cdots | B_\ell] \cdot H_f = B_f$$
$$[B_1 - x_1 G \ | \cdots | \ B_\ell - x_\ell \cdot G] \cdot H_{f,x} = B_f - f(x) \cdot G$$
- Suppose that $f : \{0,1\}^\ell \to \mathbb{Z}_q^{n \times m}$ is a matrix-valued function. Then, we will describe an analogous relation:
$$[B_1 | \cdots | B_\ell] \cdot H_f = B_f$$
$$[B_1 - x_1 G \ | \cdots | \ B_\ell - x_\ell \cdot G] \cdot H_{f,x} - f(x) \quad \text{where} \quad x = (x_1, \ldots, x_\ell)$$
- We take a bit by bit approach.
  Let $f_{j,k} : \{0,1\}^\ell \to \{0,1\}$ be function that computes k^{th} bit of j^{th} entry of $f(x)$

  Then, $[B_1 - x_1 G \ | \cdots | \ B_\ell - x_\ell G] \cdot H_{f_{j,k}, x} = B_{f_{j,k}} - [f(x)]_{j,k} \cdot G$ input-dependent evaluation

  k^{th} bit of j^{th} element of $f(x)$

  $$= [B_1 | \cdots | B_\ell] \cdot H_{f_{j,k}} - [f(x)]_{j,k} \cdot G$$

  Let $E_j \in \mathbb{Z}_q^{n \times m}$ be the matrix that is 1 in position j (where j ranges over <u>all</u> $n \cdot m$ indices)

  Then, we can write $f(x) = \sum_{j \in [n \cdot m]} \sum_{k \in [\log q]} [f(x)]_{j,k} \cdot 2^k E_j$

  bits of $f(x)$