To obtain NIZK for circular-secure FHE, suffices to show that BadChallenge function for Blum's protocol is <u>efficiently-searchable</u> (given a trapdoor)

<u>prover</u> | <u>verifier</u>

1. Sample random permutation
$$\pi \xleftarrow{R} \mathrm{Perm}[V]$$
2. Commit to edges in the permuted graph
$$\forall i,j \in [n]: \text{ if } (i,j) \in E,\ c_{\pi(i),\pi(j)} \leftarrow \mathrm{Commit}(1)$$
$$\text{else},\ c_{\pi(i),\pi(j)} \leftarrow \mathrm{Commit}(0)$$

in addition, commit to permutation π:
$$c_\pi \leftarrow \mathrm{Commit}(\pi)$$

We can define the commitment to be a GSW encryption of the message. The opening is the encryption randomness:
$$pk = A = \begin{bmatrix} \bar{A} \\ \bar{s}^T \bar{A} + e^T \end{bmatrix} \qquad sk = s = [-\bar{s} \mid 1]$$

$$\mathrm{Commit}(pk, m): R \xleftarrow{R} \{0,1\}^{m \times m}$$
$$C \leftarrow AR + \mu \cdot G$$
C is commitment
R is opening

$$\xrightarrow{\ \{c_{i,j}\}_{i,j \in [n]},\ c_\pi\ }$$

$$b \xleftarrow{R} \{0,1\}$$

$$\xleftarrow{\ b\ }$$

if $b = 0$: reveal π and open all $c_{i,j}$, c_π
if $b = 1$: open <u>only</u> the edges corresponding to the Hamiltonian cycle

$$\xrightarrow{\hspace{3cm}}$$

To open, verifier checks that
$$C = AR + \mu \cdot G \text{ and } R \in \{0,1\}^{m \times m}$$
<u>Statistically binding</u>: if $C = AR_1 + G = AR_2$ for $R_1, R_2 \in \{0,1\}^{m \times m}$, then $\underbrace{s^T A(R_1 - R_2)}_{e^T(R_1 - R_2)} = s^T G$

$$e^T(R_1 - R_2) = s^T G$$
Contradiction!

Computing the BadChallenge function efficiently:

$\mathrm{BadChallenge}(sk, (\{c_{i,j}\}, c_\pi))$:

1. Use sk to extract edges $e_{i,j} \in \{0,1\}$ from $c_{i,j}$ and $\pi \in \mathrm{Perm}[E]$ from c_π
2. Check if $e_{i,j}$ is consistent with $\pi(E)$
3. Output $b = 1$ if extraction succeeds and consistency check passes
   Output $b = 0$ otherwise

For a false instance, if $\{c_{i,j}\}, c_\pi$ are commitments to a permuted graph, then there is no Hamiltonian cycle so prover cannot answer $b = 1$ query. Otherwise if $\{c_{i,j}\}, c_\pi$ are malformed, then it cannot answer $b = 0$ query.

<u>Implication</u>: NIZK for NP from circular-secure FHE.

<u>Next</u>: Can we do it without circular security (e.g., from plain LWE)?
YES! Will do so algebraically (starting from homomorphic commitments).

Some notation: Given $B_1, \dots, B_\ell$, $f: \{0,1\}^\ell \to \{0,1\}$, we can write
$$[B_1 | \cdots | B_\ell] \cdot H_f = B_f$$
$$[B_1 - x_1 G | \cdots | B_\ell - x_\ell G] \cdot H_{f,x} = B_f - f(x) \cdot G$$
If $g: \{0,1\}^\ell \to \{0,1\}^t$ has t-bit outputs, we can write $g_1, \dots, g_t : \{0,1\}^\ell \to \{0,1\}$ to denote the function that computes the i^{th} output bit of $g(x)$
$$[B_1 | \cdots | B_\ell] \cdot [H_{g_1} | \cdots | H_{g_t}] = [B_{g_1} | \cdots | B_{g_t}]$$
$$[B_1 - x_1 G | \cdots | B_\ell - x_\ell G] \cdot [H_{g_1,x} | \cdots | H_{g_t,x}] = [B_{g_1} - g_1(x) \cdot G | \cdots | B_{g_t} - g_t(x) \cdot G]$$
We will write this more compactly as
$$H_g = [H_{g_1} | \cdots | H_{g_t}] \text{ and } B_g = [B_{g_1} | \cdots | B_{g_t}]$$
$$H_{g,x} = [H_{g_1,x} | \cdots | H_{g_t,x}]$$

view $g(x)$ as vector
$[g_1(x) | \cdots | g_t(x)] \in \{0,1\}^t$

$$[B_{g_1} - g_1(x) \cdot G | \cdots | B_{g_t} - g_t(x) \cdot G] = B_g - [g_1(x) \cdot G | \cdots | g_t(x) \cdot G] = B_g - g(x) \otimes G$$

Lattice homomorphisms for multi-bit functions $g : \{0,1\}^\ell \to \{0,1\}^t$:

$$[B_1 | \cdots | B_\ell] \cdot H_g = B_g$$
$$[B_1 - x_1 G | \cdots | B_\ell - x_\ell \cdot G] \cdot H_{g,x} = B_g - g(x) \otimes G$$

Kronecker / tensor product

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix}, \quad A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nm}B \end{bmatrix}$$

$k = n \lfloor \log q \rfloor$

Setup (1^λ): Sample $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$ and $R_1, \ldots, R_\ell \xleftarrow{R} \{0,1\}^{m \times k}$ and $b \xleftarrow{R} \mathbb{Z}_q^n$ [ℓ is description length of function f]

Let $B_1 \leftarrow AR_1, \ldots, B_\ell \leftarrow AR_\ell$. [commitment to all-zeroes string]

Output $hk = (b, B_1, \ldots, B_\ell)$

Hash(hk, x): Compute $B_{u_x} = [B_1 | \cdots | B_\ell] \cdot H_{u_x} \in \mathbb{Z}_q^{n \times k^2}$ [$u_x : \{0,1\}^\ell \to \{0,1\}^k$, $f \mapsto f(x)$]

Output $G^{-1}(b + B_{u_x} \cdot G^{-1}(z))$ for some vector $z \in \mathbb{Z}_q^{nk}$ to be determined (fixed and public)

To argue correlation-intractability, we use a hybrid argument:

Hyb$_0$: real game

Hyb$_1$: replace $B_1 \leftarrow AR_1 + f_1 G, \ldots, B_\ell \leftarrow AR_\ell + f_\ell \cdot G$ (where $f_1, \ldots, f_\ell$ are bits of f) commitment to the bits of f

Hyb$_0 \overset{s}{\approx}$ Hyb$_1$ by leftover hash lemma

In Hyb$_1$, suppose adversary can find x such that Hash$(hk, x) = f(x)$. Then,

$$f(x) = \text{Hash}(hk, x) = G^{-1}(b + B_{u_x} \cdot G^{-1}(z))$$ $\leftarrow$ view $f(x) \in \{0,1\}^m$ as a vector

$$\Rightarrow G \cdot f(x) = b + B_{u_x} \cdot G^{-1}(z)$$ $\leftarrow$ $B_{u_x} = [B_1 | \cdots | B_\ell] \cdot H_{u_x}$

$$= b + [B_1 - f_1 G | \cdots | B_\ell - f_\ell \cdot G] H_{u_x,f}\, G^{-1}(z) + (f(x) \otimes G) \cdot G^{-1}(z)$$

$[B_1 - f_1 G | \cdots | B_\ell - f_\ell G] \cdot H_{u_x,f} = B_{u_x} - u_x(f) \otimes G = B_{u_x} - f(x) \otimes G$

$$= b + \underbrace{A[R_1 | \cdots | R_\ell] \cdot H_{u_x,f}}_{\text{short}} G^{-1}(z) + \underbrace{(f(x) \otimes G) \cdot G^{-1}(z)}_{\text{suppose this is equal to } G \cdot f(x)}$$

$\Rightarrow A[R_1 | \cdots | R_\ell] \cdot H_{u_x,f} + b = 0$

with A, b random $\Rightarrow$ SIS solution!

Goal: Choose z such that $(f(x) \otimes G) \cdot G^{-1}(z)$

Rearrange components of z:

$$z = \begin{bmatrix} z_1 & z_2 & \cdots & z_n \\ z_{n+1} & z_{n+2} & \cdots & z_{2n} \\ \vdots & \vdots & & \vdots \\ z_{(k-1)n+1} & z_{(k-1)n+2} & & z_{nk} \end{bmatrix}$$ $\leftarrow$ denote this matrix $Z \in \mathbb{Z}_q^{k \times n}$; let Z_i^T denote the i^{th} row of Z (as a column vector)

Let $f^{(i)}(x)$ denote i^{th} bit of output of $f(x)$

$$\underbrace{[f^{(1)}(x) \cdot G | \cdots | f^{(k)}(x) \cdot G]}_{f(x) \otimes G} \cdot G^{-1}(z) = [\underbrace{f^{(1)}(x) \cdot G}_{\in \mathbb{Z}_q^{n \times k}} | \cdots | \underbrace{f^{(k)}(x) \cdot G}_{\in \mathbb{Z}_q^{n \times k}}] \cdot \begin{bmatrix} G^{-1}(Z_1^T) \\ \vdots \\ G^{-1}(Z_k^T) \end{bmatrix} \begin{matrix} \} \in \mathbb{Z}_q^k \\ \\ \} \in \mathbb{Z}_q^k \end{matrix}$$

$$= f^{(1)}(x) \cdot G \cdot G^{-1}(Z_1^T) + \cdots + f^{(k)}(x) \cdot G \cdot G^{-1}(Z_k^T)$$

$$= \sum_{i \in [k]} f^{(i)}(x) \cdot Z_i^T$$ linear combination of rows of Z = linear combination of columns of Z^T

$$= Z^T \cdot f(x)$$

Choose z so that associated matrix $Z = G^T$. Then

$$(f(x) \otimes G) \cdot G^{-1}(z) = G \cdot f(x)$$

Key property: for any matrix M, we can construct vector m such that
$$(x^T \otimes G) \cdot G^{-1}(M) = M \cdot x$$
for any vector x (assuming proper dimensions)

Then, $\mathrm{Hash}(hk, x) = G^{-1}(b + B_{u_x} \cdot G^{-1}(z))$

To reduce to SIS, let $[A \mid b]$ be SIS challenge.
Set $B_1 = AR_1 + f_1 G, \ldots, B_\ell = AR_\ell + f_\ell \cdot G$
Output $hk = (b, B_1, \ldots, B_\ell)$

Suppose adversary outputs x such that $f(x) = \mathrm{Hash}(hk, x)$.
Then,

$$\begin{aligned} G \cdot f(x) &= G \cdot G^{-1}(b + B_{u_x} \cdot G^{-1}(z)) \\ &= b + B_{u_x} \cdot G^{-1}(z) \end{aligned}$$

Now $AR_1 = B_1 - f_1 G, \ldots, AR_\ell = B_\ell - f_\ell \cdot G$

$$\underbrace{[B_1 - f_1 G \mid \cdots \mid B_\ell - f_\ell \cdot G]}\, H_{u_x, f} = B_{u_x} - f(x) \otimes G$$

$$A[R_1 \mid \cdots \mid R_\ell] \cdot H_{u_x, f} = B_{u_x} - f(x) \otimes G$$

$$\Rightarrow B_{u_x} = A[R_1 \mid \cdots \mid R_\ell] \cdot H_{u_x, f} + f(x) \otimes G$$

Thus,

$$\begin{aligned} G \cdot f(x) &= b + B_{u_x} \cdot G^{-1}(z) \\ &= b + A[R_1 \mid \cdots \mid R_\ell] \cdot H_{u_x, f} \cdot G^{-1}(z) + (f(x) \otimes G) \cdot G^{-1}(z) \\ &= b + A[R_1 \mid \cdots \mid R_\ell] \cdot H_{u_x, f} \cdot G^{-1}(z) + G \cdot f(x) \end{aligned}$$

$$\Rightarrow \underbrace{A[R_1 \mid \cdots \mid R_\ell] \cdot H_{u_x, f} \cdot G^{-1}(z)} + b = 0$$

small since $R_1, \ldots, R_\ell, G^{-1}(z)$ are binary, $\|H_{u_x, f}\| = (n \log q)^{O(\log d)}$ where d is the depth of the computation

This yields a correlation-intractable hash function for all search relations from SIS
↳ NIZK for NP from LWE (LWE used for extractable commitment)

this requires a large modulus $q \sim (n \log q)^{O(d)}$, but can reduce to $q \sim \mathrm{poly}(n)$ when considering log-depth circuits (via branching programs)

↓

can then bootstrap to $\mathrm{poly}(\lambda)$ depth using (leveled) FHE $\Rightarrow$ correlation-intractable hash function for all search relations from LWE with polynomial modulus