Recall: trapdoor for B is short matrix R where $BR = G$. Allows sampling short solutions to $Bx = y$ for any $y \in \mathbb{Z}_q^{\ell n}$.

Note: unclear how to use trapdoor for B to solve SIS with respect to A:

$$\begin{bmatrix} A & & & W_1 \\ & \ddots & & \vdots \\ & & A & W_\ell \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_\ell \\ x^* \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_\ell \end{bmatrix} \implies A x_i + W_i x^* = y_i$$

can sample using R

$$A x_i = y_i - W_i x^*$$

can obtain preimage of $y_i - W_i x^*$ but no control over x^*

Compressing GVW commitments: previously, we had

$$C_1 = AR_1 + x_1 G$$
$$\vdots$$
$$C_\ell = AR_\ell + x_\ell G$$

commitment is $(C_1, \ldots, C_\ell)$ $\downarrow$ compress to single C

Suppose we defined $C_i = W_i C$ where $C \in \mathbb{Z}_q^{m \times m}$. Then, the above relations become

$$\begin{aligned} W_1 C &= AR_1 + x_1 G \\ &\vdots \\ W_\ell C &= AR_\ell + x_\ell G \end{aligned} \implies \begin{aligned} AR_1 - W_1 C &= -x_1 G \\ &\vdots \\ AR_\ell - W_\ell C &= -x_\ell G \end{aligned}$$

$$\Downarrow$$

$$\begin{bmatrix} A & & & W_1 \\ & \ddots & & \vdots \\ & & A & W_\ell \end{bmatrix} \begin{bmatrix} R_1 \\ \vdots \\ R_\ell \\ C \end{bmatrix} = \begin{bmatrix} -x_1 G \\ \vdots \\ -x_\ell G \end{bmatrix}$$

can sample using a trapdoor!

Idea: public parameters for commitment scheme is (A, B, R) where $BR = G$.
to commit, compute

$$\begin{bmatrix} R_1 \\ \vdots \\ R_\ell \\ C \end{bmatrix} = \underbrace{\begin{bmatrix} A & & & W_1 \\ & \ddots & & \vdots \\ & & A & W_\ell \end{bmatrix}}_{B}^{-1} \left(\begin{bmatrix} -x_1 G \\ \vdots \\ -x_\ell G \end{bmatrix} \right) \implies AR_i + W_i C = -x_i G$$

commitment to $x \in \{0,1\}^\ell$ is $C \in \mathbb{Z}_q^{m \times m}$ (independent of ℓ).
opening to function f is

$$R_{f, f(x)} = [R_1 | \cdots | R_\ell] \cdot H_{f,x}$$

to check the commitment and opening, verifier first computes $C_i = -W_i C \in \mathbb{Z}_q^{n \times m}$ and computes C_f from $C_1, \ldots, C_\ell$ as in GVW and then checks that

$$C_f = AR_{f, f(x)} + f(x) \cdot G$$

correctness follows from key equation:

$$\begin{aligned} AR_{f, f(x)} = [AR_1 | \cdots | AR_\ell] \cdot H_{f,x} &= [-W_1 C - x_1 G | \cdots | -W_\ell C - x_\ell G] \cdot H_{f,x} \\ &= [C_1 - x_1 G | \cdots | C_\ell - x_\ell G] \cdot H_{f,x} \\ &= C_f - f(x) \cdot G \end{aligned}$$

Binding (from ℓ-succinct SIS): Suppose adversary can find commitment C, function f, and openings R_0, R_1 where

$$C_f = AR_0 \quad \text{and} \quad C_f = AR_1 - G \quad \text{where } R_0, R_1 \text{ are short}$$

Then $0 = A(R_1 - R_0) - G$ or $A(R_1 - R_0) = G$.

Thus, $R_1 - R_0$ is a trapdoor for A and breaks SIS with respect to A.

Note: ℓ-succinct SIS needed to simulate public parameters (i.e., trapdoor for B).