Define

- A special parity-check matrix: let $\mathbf{g}^t = [1\ 2\ 4\ \cdots\ 2^{k-1} \geq \frac{q}{2}]$ and

$$\mathbf{G} = \begin{bmatrix} \cdots\mathbf{g}^t\cdots & & & \\ & \cdots\mathbf{g}^t\cdots & & \\ & & \ddots & \\ & & & \cdots\mathbf{g}^t\cdots \end{bmatrix} \in \mathbb{Z}_q^{n\times nk}.$$

# Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t\mathbf{A} \approx \mathbf{0}$.

# Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t \mathbf{A} \approx \mathbf{0}$.
- Encrypt $\mu \in \{0, 1\}$ as $\mathbf{C} = \mathbf{AR} + \mu \mathbf{G}$. Decryption relation is

$$\mathbf{s}^t \mathbf{C} \approx \mu \cdot \mathbf{s}^t \mathbf{G}.$$

# Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t\mathbf{A} \approx \mathbf{0}$.
- Encrypt $\mu \in \{0, 1\}$ as $\mathbf{C} = \mathbf{AR} + \mu\mathbf{G}$. Decryption relation is

$$\mathbf{s}^t\mathbf{C} \approx \mu \cdot \mathbf{s}^t\mathbf{G}.$$

- Homomorphic mult: $\mathbf{C}_\times = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2)$.

# Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t\mathbf{A} \approx \mathbf{0}$.
- Encrypt $\mu \in \{0, 1\}$ as $\mathbf{C} = \mathbf{AR} + \mu\mathbf{G}$. Decryption relation is

$$\mathbf{s}^t\mathbf{C} \approx \mu \cdot \mathbf{s}^t\mathbf{G}.$$

- Homomorphic mult: $\mathbf{C}_\times = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2)$.

$$\begin{aligned}\mathbf{s}^t\mathbf{C}_\times &= \mathbf{s}^t\mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &\approx \mu_1 \cdot \mathbf{s}^t\mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &\approx \mu_1\mu_2 \cdot \mathbf{s}^t\mathbf{G}\end{aligned}$$

## Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t\mathbf{A} \approx \mathbf{0}$.
- Encrypt $\mu \in \{0, 1\}$ as $\mathbf{C} = \mathbf{A}\mathbf{R} + \mu\mathbf{G}$. Decryption relation is

$$\mathbf{s}^t\mathbf{C} \approx \mu \cdot \mathbf{s}^t\mathbf{G}.$$

- Homomorphic mult: $\mathbf{C}_\times = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2)$.

$$\begin{aligned} \mathbf{s}^t\mathbf{C}_\times &= \mathbf{s}^t\mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &\approx \mu_1 \cdot \mathbf{s}^t\mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &\approx \mu_1\mu_2 \cdot \mathbf{s}^t\mathbf{G} \end{aligned}$$

  Error in $\mathbf{C}_\times$ is $\mathbf{e}_1^t \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + \mu_1 \cdot \mathbf{e}_2^t$.

  Asymmetry allows homom mult with additive noise growth. [BV'13]