参数 n 是格的维数，χ 是 $\mathbb{Z}$ 上的噪音高斯分布，其值选取的尽可能小，素整数 $q=q(n)$ 是模。

E1.SecretKeygen(1^n)：随机均匀选取向量 $\boldsymbol{s}' \leftarrow \mathbb{Z}_q^n$，输出 $sk = \boldsymbol{s} \leftarrow (1, \boldsymbol{s}') \in \mathbb{Z}_q^{n+1}$。

E1.PublicKeygen($\boldsymbol{s}$): 令 $N \geqslant 2(n\log q)$。随机均匀选取矩阵 $\boldsymbol{A}' \leftarrow \mathbb{Z}_q^{N\times n}$ 和向量 $\boldsymbol{e} \leftarrow \chi^N$。计算 $\boldsymbol{b} \leftarrow \boldsymbol{A}'\boldsymbol{s}' + \boldsymbol{e}$。令 $\boldsymbol{A}$ 是 n+1 列矩阵，由向量 $\boldsymbol{b}$ 和矩阵$-\boldsymbol{A}'$构成，即 $\boldsymbol{A} = [\boldsymbol{b} | -\boldsymbol{A}'] \in \mathbb{Z}_q^{N\times(n+1)}$，其中 $\boldsymbol{A}\cdot\boldsymbol{s} = \boldsymbol{e}$。输出 $pk = \boldsymbol{A}$。

E1.Enc(pk, m)：为了加密消息 $m \in \{0,1\}$，令 $\boldsymbol{m} \leftarrow (m, 0, \cdots, 0) \in \{0,1\}^{n+1}$。选取 $\boldsymbol{r} \in \{0,1\}^N$，输出密文 $\boldsymbol{c} \leftarrow \lfloor q/2 \rfloor \cdot \boldsymbol{m} + \boldsymbol{A}^T \cdot \boldsymbol{r} \in \mathbb{Z}_q^{n+1}$。

E1.Dec(sk, c)：输出 $m \leftarrow \lfloor \frac{2}{q}[<\boldsymbol{c}, \boldsymbol{s}>]_q \rceil \bmod 2$。

解密正确性条件：该方案密文解密的正确性条件是：密文中的噪音小于 $\lfloor q/2 \rfloor / 2$ 时，密文可以被正确解密。