Parameters: Our goal is to generate k hidden-bits. $N = \Theta(k^\delta), \delta \in (0,1)$. The exact weight w is specifically chosen to ensure a proper minimum distance in exact-LPN. Denote Gaussian noise distribution with $\mathcal{B}_\mu^N$ and exact-weight noise distribution with X_w^N.

- **Setup**(1^k):
  1. $\forall i \in [k], A_i \xleftarrow{\$} \{0,1\}^{N\times N},\ s_i \xleftarrow{\$} \{0,1\}^N,\ e_i \leftarrow \mathcal{B}_\mu^N$.
  2. Decide w, weight parameter for exact-LPN.
  3. Compute $b_i := A_i \cdot s_i + e_i$.
  4. Sample $\alpha \xleftarrow{\$} \{0,1\}^{N\times N}$ (for hiding seed)
  5. $\mathsf{crs} := \{\{(A_i, b_i) \mid i \in [k]\}, w, \alpha\}$, $\mathsf{td} := \{s_i \mid i \in [k]\}$.
- **Genbits**$(1^k, \mathsf{crs})$:
  1. $\mathit{seed} \xleftarrow{\$} \{0,1\}^N, \epsilon \leftarrow \mathcal{B}_\mu^N$, hide *seed* as $\beta := \alpha \cdot \mathit{seed} + \epsilon$.
  2. $\forall i \in [k],\ e'_i \leftarrow \{0,1\}^N$, compute $b'_i := A_i \cdot \mathit{seed} + e'_i$.
  3. Compute hidden-bits $r_i := \mathsf{hc}(b_i; \mathit{seed}),\ \forall i \in [k]$.
  4. Sample $x \xleftarrow{\$} \{0,1\}^{N-1},\ \forall i \in [k],\ \eta_i \leftarrow X_w^N$ s.t. $|\eta_i| = w$.
  5. Compute $B_i := A_i \cdot (x \| r_i) + \eta_i$.
  6. $\mathsf{com} := \{x, \beta\},\ \pi_i := \{b'_i, B_i\},\ \forall i \in [k]$.
- **Verify**$(1^k, \mathsf{crs}, \mathsf{com}, i, \pi_i, r, \mathsf{td}_i)$:
  1. Check $r = \mathsf{hc}(\pi_{i,1}; \mathsf{td}_i)$ i.e. $r = \mathsf{hc}(b'_i; s_i)$.
  2. Check $|\pi_{i,2} \oplus A_i \cdot (\mathsf{com}_1 \| r)| = w$ i.e. $|B_i \oplus A_i \cdot (x\|r)| = w$
  3. But how do we validate $\mathsf{com}_2 = \beta$? Or can we prove cheating β will not hurt binding?
  4. Accept if and only if all the above hold.
- **Open**$(1^k, \mathsf{crs}, \mathsf{com})$: Inefficiently solve LPN sample β to get *seed*, then compute all hidden bits from $r_i := \mathsf{hc}(b_i; \mathit{seed}),\ \forall i \in [k]$.

There is an error probability because of hardcore computation, which can be reduced to negligible by limiting noise rate.