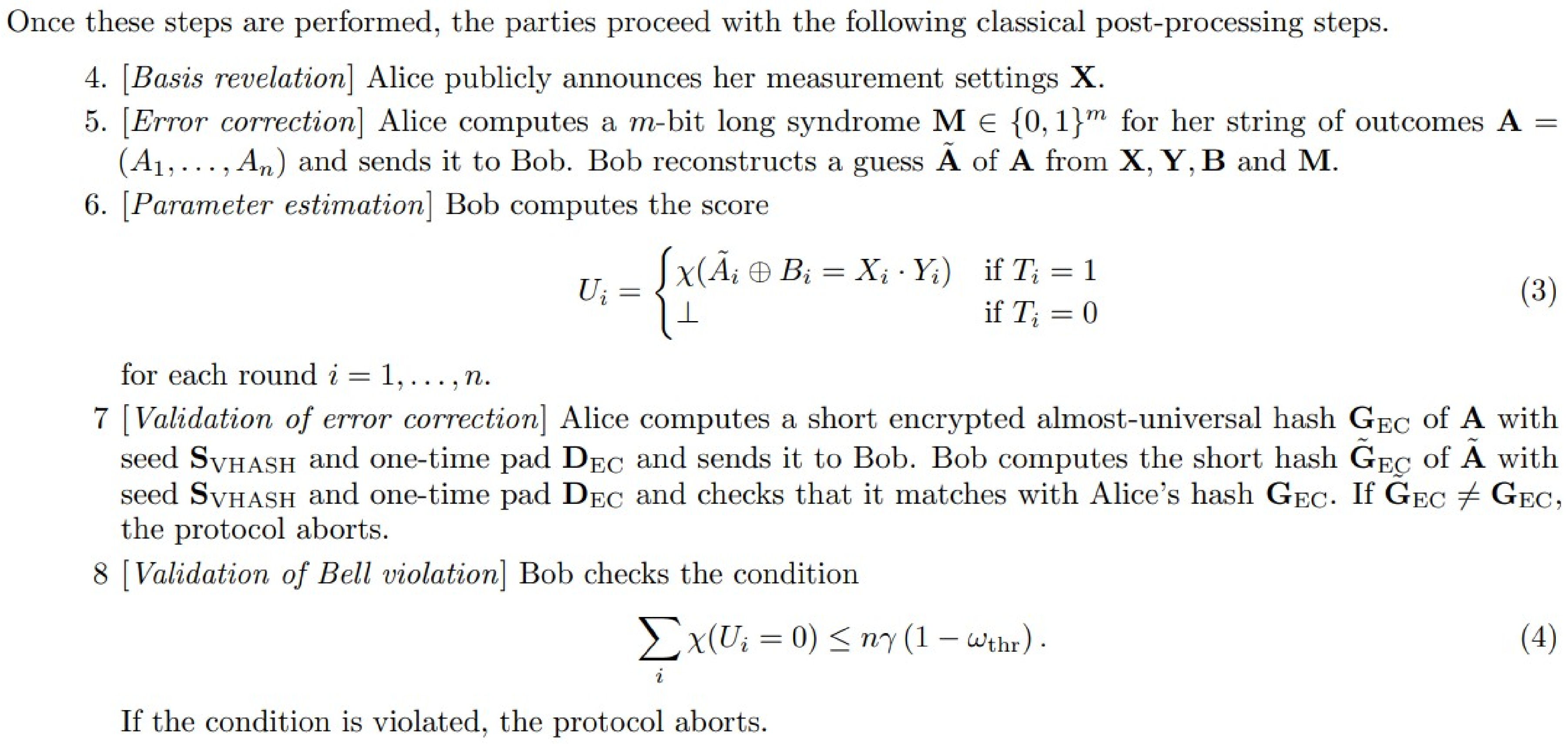
Key unification/verification in DIQKD



Once these steps are performed, the parties proceed with the following classical post-processing steps.

4. [*Basis revelation*] Alice publicly announces her measurement settings $\mathbf{X}$.
5. [*Error correction*] Alice computes a m-bit long syndrome $\mathbf{M} \in \{0,1\}^m$ for her string of outcomes $\mathbf{A} = (A_1, \ldots, A_n)$ and sends it to Bob. Bob reconstructs a guess $\tilde{\mathbf{A}}$ of $\mathbf{A}$ from $\mathbf{X}, \mathbf{Y}, \mathbf{B}$ and $\mathbf{M}$.
6. [*Parameter estimation*] Bob computes the score

$$U_i = \begin{cases} \chi(\tilde{A}_i \oplus B_i = X_i \cdot Y_i) & \text{if } T_i = 1 \\ \perp & \text{if } T_i = 0 \end{cases} \tag{3}$$

for each round $i = 1, \ldots, n$.

7 [*Validation of error correction*] Alice computes a short encrypted almost-universal hash $\mathbf{G}_{\text{EC}}$ of $\mathbf{A}$ with seed $\mathbf{S}_{\text{VHASH}}$ and one-time pad $\mathbf{D}_{\text{EC}}$ and sends it to Bob. Bob computes the short hash $\tilde{\mathbf{G}}_{\text{EC}}$ of $\tilde{\mathbf{A}}$ with seed $\mathbf{S}_{\text{VHASH}}$ and one-time pad $\mathbf{D}_{\text{EC}}$ and checks that it matches with Alice's hash $\mathbf{G}_{\text{EC}}$. If $\tilde{\mathbf{G}}_{\text{EC}} \neq \mathbf{G}_{\text{EC}}$, the protocol aborts.

8 [*Validation of Bell violation*] Bob checks the condition

$$\sum_i \chi(U_i = 0) \leq n\gamma\left(1 - \omega_{\text{thr}}\right). \tag{4}$$

If the condition is violated, the protocol aborts.

Key unification

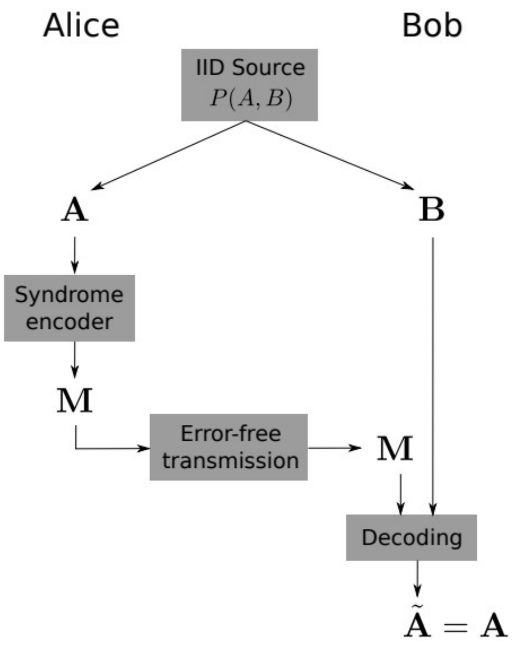


Fig. S8: Overall error correction setting: asymmetric Slepian-Wolf coding. Strings **A** and **B** are jointly sampled from a distribution $P(A, B)$ and given to two distinct parties Alice and Bob. The aim is for Bob to end up with a copy of Alice's string **A**, while only exchanging a 'short' message **M**.

Key Unification

- **4. One-way error correction and verification:** In the first part, Alice computes a syndrome based on her raw key (denoted by L) and sends it to Bob via the public channel, who then uses the syndrome and his raw key to recover Alice’s key. In the second part, they perform an error verification by comparing the hash values of their raw keys. Alice and Bob proceed to privacy amplification if the hash values are identical, otherwise they abort the protocol.

Code

- low-density parity-check (LDPC) codes, spatially-coupled LDPC (SC-LDPC) codes and polar codes