The present invention relates to a method and an apparatus for quantum key distribution according to a continuous-variable quantum key distribution protocol, which distributes the quantum key in a reverse post-processing manner and, after photon subtraction at a receiver (Bob), detects bit information from a received quantum state to calculate and share the quantum key, such that security can be further enhanced and a cryptographic key generation rate can be increased since the cryptographic key is not exposed to an attacker (Eve).