This work is focused on the description of one verifiable encryption scheme, specifically a zero-knowledge proof of knowledge protocol. Verifiable encryption allows us to prove properties of data without revealing its content. The main goal of the presented method is verification of knowledge of a secret key. This method can be used for group signatures, multiple steps secret sharing, key escrow protocols, and many others cryptographic protocols. It is based on the hardness of the Ring-LWE problem and problems of finding solutions to linear relations over some ring. It uses the principle of rejection sampling. The method is build on two closely described cryptographic protocols, Ring-LWE and Fiat-Shamir with aborts. It uses the construction of polynomial rings $R = Z[x]/(x^n + 1)$ a $R_q = Z_q[x]/(x^n + 1)$.