Práce se zaměřuje na popis kryptografického protokolu, který se řadí do skupiny ověřitelného šifrování, přesněji jde o metodu ověření s nulovou znalostí. Ověřitelné šifrování nám dovoluje dokázat vlastnosti určitého textu. Pokud je šifrovací schéma je bezpečné, nemělo by při důkazu dojít k prozrazení obsahu textu. Hlavním cílem metody je ověření znalosti soukromého klíče. Metodu lze využít k vytváření skupinových podpisů, předávání informací ve více krocích, nebo například k uschovávání klíčů. Je založena na složitosti okruhového-LWE šifrování v kombinaci s hledáním řešení soustav lineárních rovnic a využívá principu *rejection sampling*. Zkoumaná metoda spojuje principy dvou blíže popsaných kryptografických metod a to okruhového LWE a metody. Využívá konstrukci faktorokruhů $R = \mathbb{Z}[x]/(x^n + 1)$ a $R_q = \mathbb{Z}_q[x]/(x^n + 1)$.