

Cílem práce je prozkoumat možnosti implementace uživatelsky přívětivého a praktického kryptosystému založeného na algoritmech neohrožitelných kvantovými počítači. Předpokládá se co nejširší nasazení kryptografie založené na samoopravných kódech (McEliece kryptosystém) a zachování podobnosti s existujícími kryptografickými aplikacemi (GnuPG).