V práci studujeme popiratelné šifrování, které navrhli Canetti et al. (CRYPTO 1997). Běžná šifrovací schémata zaručují dobrou úroveň bezpečnosti, avšak pokud může útočník přinutit odesílatele a/nebo příjemce zprávy k odtajnění svých neveřejných informací, tato schémata selhávají. Pokud útočník zná správný šifrový text, tajné vstupy ve většině případů zavazují uživatele ke skutečnému otevřenému textu. Popiratelné šifrování poskytuje algoritmy, které umožní vyrobit alternativní tajnou informaci, jež útočníka přesvědčí o tom, že byl zašifrován jiný otevřený text.

Obsahem práce je představení nejdůležitějších výsledků v této oblasti, konkrétně schemata autorů Canetti et al. (CRYPTO 1997), schema autorů Klonowski et al. (SOFSEM 2008) založené na šifře ElGamal a schémata a negativní výsledek autorů Bendlin et al. (ASIACRYPT 2011). Kromě studia známých výsledků a jejich prezentace v jednotném prostředí podrobně zkoumáme schémata založená na simulovatelném šifrování. Zkonstruujeme schéma, které je bipopiratelné, a jehož obě indukovaná schémata jsou popiratelná příjemcem (ve flexibilním/vícedistribučním smyslu). Dále vyvracíme správnost konstrukce plně bipopiratelného schématu autorů Bendlin et al. (ASIACRYPT 2011) a tento výsledek ověříme počítačovou simulací. Tím se konstrukce tohoto typu schématu stává opět otevřeným problémem.