Tato diplomová práce se zabývá *jednosměrnými permutacemi s padacími dvířky odolnými vůči útočníkům s částečnou znalostí předobrazu* (PLR-TDPs) a jejich aplikacemi pro *důkazy replikovaného uložení dat* a *nekomprimovatelná kódování*. Samotná práce je rozdělena do tří kapitol, které popisují jednosměrné permutace s padacími dvířky, formální definici PLR-TDPs a analýzu bezpečnosti PLR-TDPs.

V první kapitole připomínáme definici jednosměrných permutací s padacími dvířky (TDPs) a ukazujeme jejich vlastnosti a aplikace pro důkazy replikovaného uložení dat. Naše výsledky jsou popsány ve druhé a třetí kapitole. Ve druhé kapitole formálně definujeme PLR-TDPs a s jejich pomocí konstruujeme jednoduché nekomprimovatelné kódování v modelu náhodného orákula. Ve třetí kapitole studujeme, zda PLR-TDPs existují. V idealizovaném modelu náhodných TDPs ukazujeme jejich odolnost vůči útočníkům s částečnou znalostí předobrazu. Jako první tak předkládáme částečné formální opodstatnění domněnky, že i praktické TDPs, jako například RSA či Rabinova permutace, jsou odolné vůči útočníkům s částečnou znalostí předobrazu.