This thesis explores *preimage leakage-resilient trapdoor permutations* (PLR-TDPs) and their applications in *proofs of storage replication* and *incompressible encodings*. The thesis consists of three chapters covering the trapdoor permutations, formal definition of PLR-TDPs, and analysis of security properties of PLR-TDPs.

The first chapter provides an overview of trapdoor permutations (TDPs), their definitions, and applications in proofs of storage replication. Our results are presented in the second and third chapters. The second chapter formally defines PLR-TDPs and demonstrates their use by constructing a simple incompressible encoding in the random oracle model. The third chapter focuses on the existence of PLR-TDPs. It demonstrates the strong preimage leakage-resilience of fully random TDPs in an idealized model. We are the first to provide a partial formal justification for the conjecture of the preimage leakage-resilience of practical TDPs, such as RSA or Rabin permutations.