This thesis focuses on constructions of Homomorphic Secret Sharing (HSS) based on assumptions not known to imply fully homomorphic encryption. The efficiency of these constructions depends on the complexity of the Distributed Discrete Logarithm (DDLog) problem in the corresponding groups. We describe this problem in detail, focusing on the possibility of leveraging preprocessing in prime order groups, and deriving upper bounds on the success probability for the DDLog problem with preprocessing in the generic group model. Further, we present a new HSS construction. We base our construction on the Joye-Libert encryption scheme which we adapt to support an efficient distributed discrete logarithm protocol. Our modified Joye-Libert scheme requires a new set of security assumptions, which we introduce, proving the IND-CPA security of our scheme given these assumptions.