Homomorphic Secret Sharing

A homomorphic secret-sharing scheme is a secret-sharing scheme that allows locally mapping shares of a secret to compact shares of a function of the secret. The talk will survey the current state of the art on homomorphic secret sharing, covering efficient constructions, applications in cryptography and complexity theory, and open questions.