*accept iff*

*E (0, z) = Tuc mod ns+1*

**Verifier**

**Prover**

*Offer: T = E (0,t) t🡨R Zns*

*Challenge: c random*

*Response: z = trc*

**ns - Power Protocol**

*I know v such that*

*u = E (0, r)*

**KEY GENERATION ALGORITHM**

*security parameter*

*#decryption servers*

*threshold*

*randomness*

*public key PK*

*secret keys SK1, …, SKl*

*verification keys VK1, …, VKl*

**ENCRYPTION ALGORITHM**

*public key*

*message*

*randomness*

*ciphertext*

**COMBINING ALGORITHM**

*public key*

*decryption share*

*validity proof*

*verification keys*

*plaintext or failure*

*ciphertext*

**SHARE DECRYPTION ALGORITHM**

*public key PK*

*verification key*

*secret share*

*ciphertext*

*decryption share*

*validity proof*