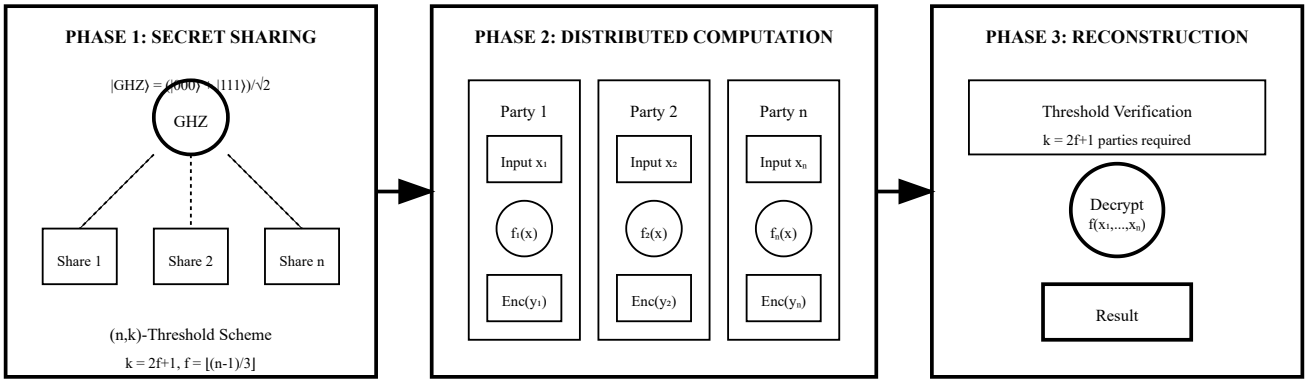
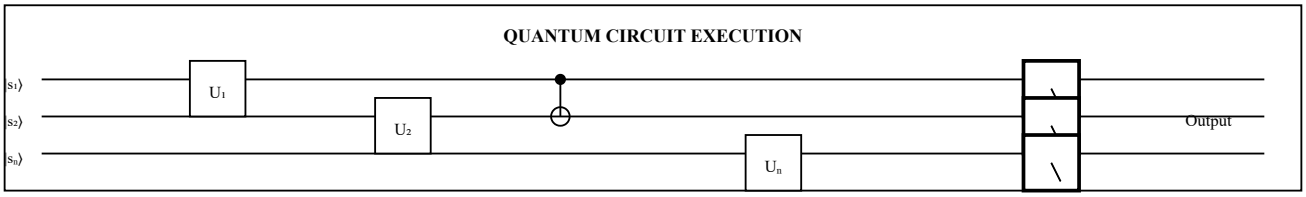
FIGURE 8: MULTI-PARTY COMPUTATION WITH SECRET SHARING AND RECONSTRUCTION



SECURITY GUARANTEES

- Privacy: No party learns others' inputs
- Correctness: Verified output
- Robustness: t less than n/3 malicious
- Information-theoretic security
- Fairness: Simultaneous output
- Quantum advantage



PROTOCOL STEPS:

1. Generate GHZ state for n parties
2. Distribute quantum shares
3. Each party computes on encrypted share
4. Homomorphic operations preserve encryption
5. k parties collaborate for decryption
6. Verify computation correctness

Secret Sharing: $|\psi\rangle = \Sigma_i |s_i\rangle$

Computation: $f(x_1,...,x_n) = \Sigma_i f_i(x_i)$

Reconstruction: $k = 2f+1$, $f = \lfloor (n-1)/3 \rfloor$