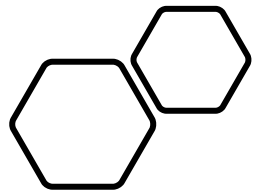


# Quantum Secure Multiparty Computation of Phylogenetic Trees

Manuel Santos, Ana C. Gomes, Armando Nolasco  
Pinto, Paulo Mateus

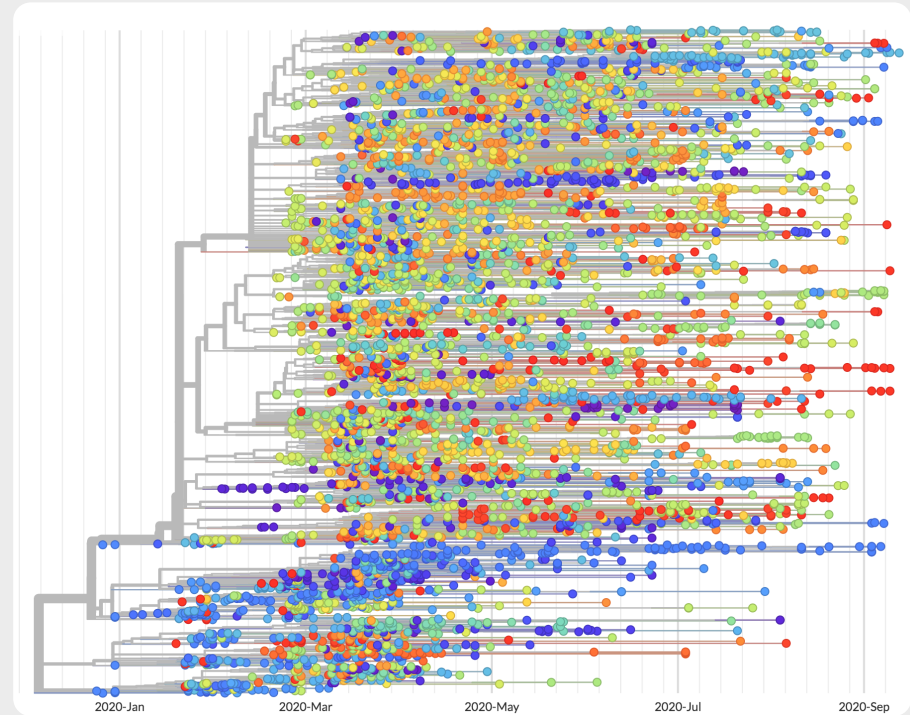
Instituto Superior Técnico  
Universidade de Aveiro  
Instituto de Telecomunicações  
CBRA Genomics



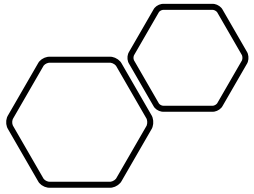


# Phylogenetic Trees

- Show the evolutionary relationship between DNA sequences of the same/different specie in a tree.
- Also known as **Evolutionary Tree**.
- Algorithms:
  - Character-based.
  - Distance-based: Unweighted pair group method with arithmetic mean (UPGMA).



Source: GISAID



# UPGMA

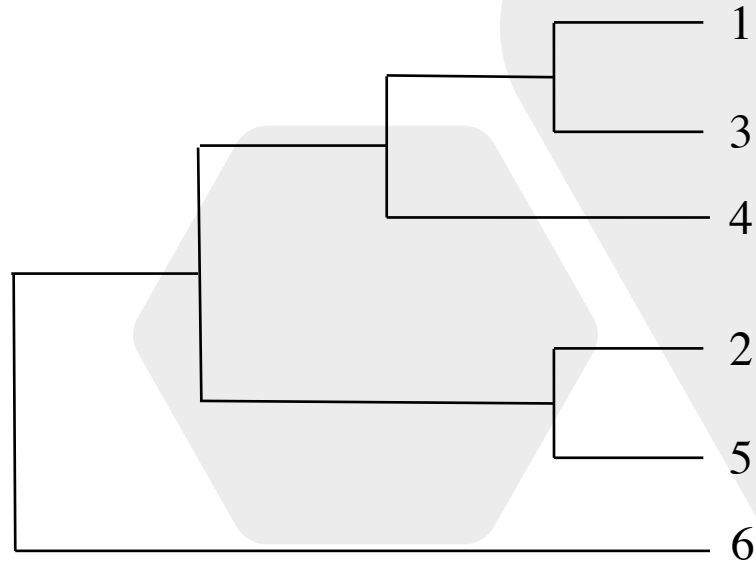


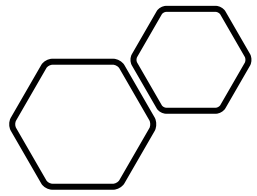
Part 1: Compute the distance matrix.



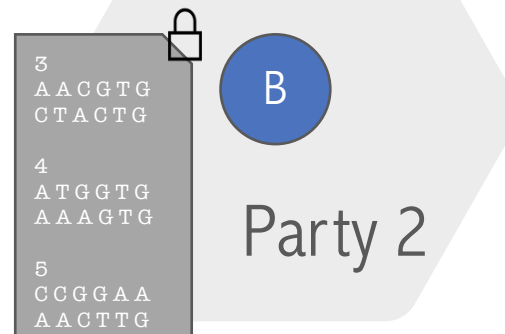
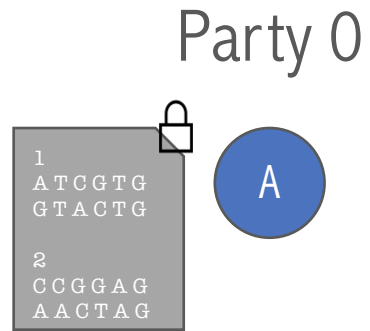
Part 2: Iteratively group the genes with the fewest differences between them.

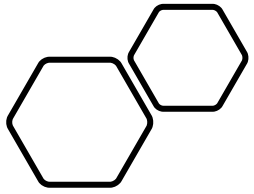
Final output:



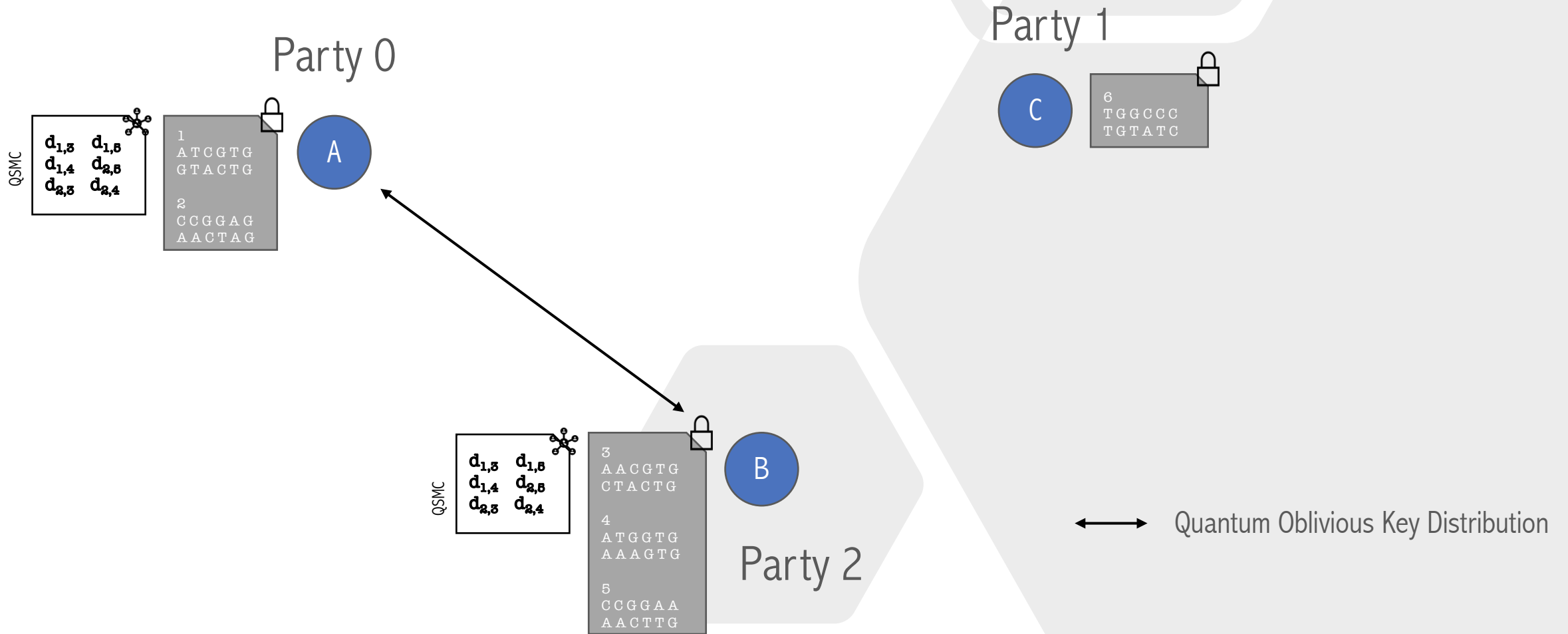


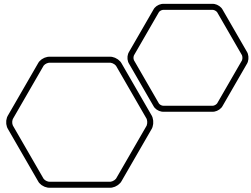
# System Design — Private UPGMA



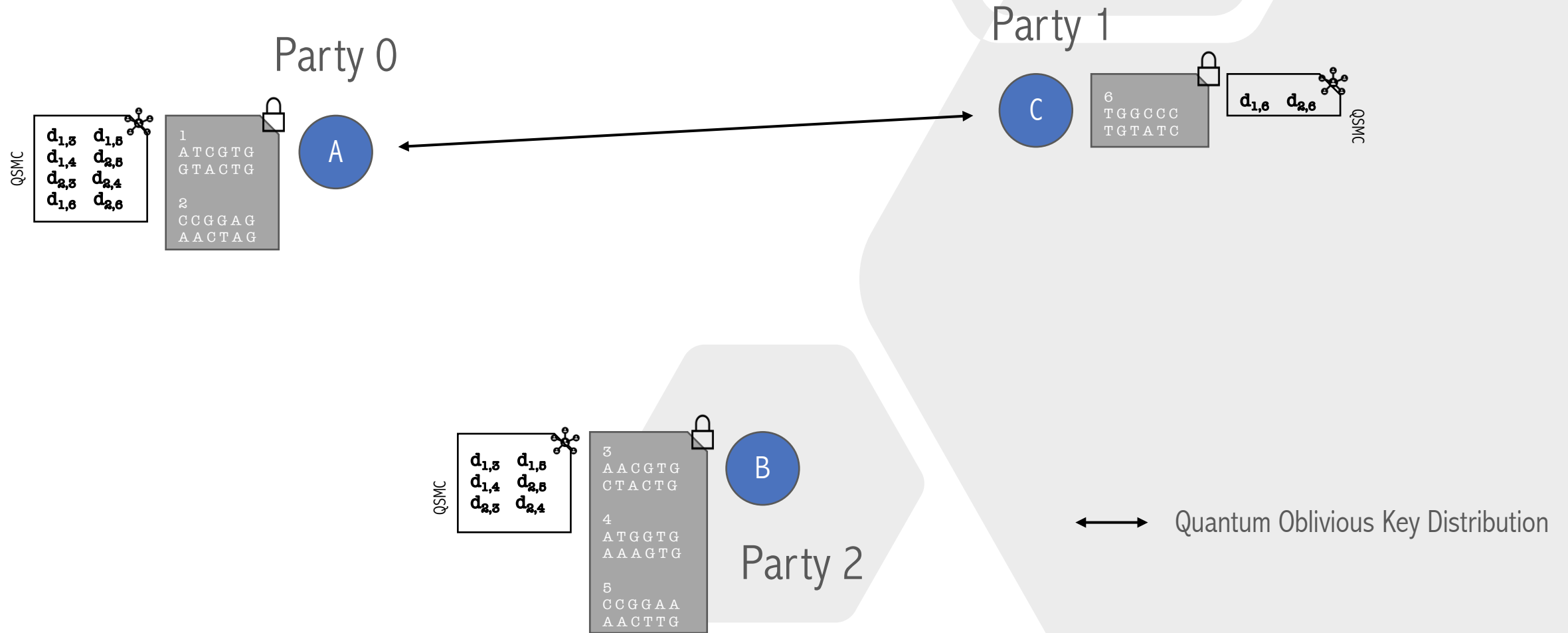


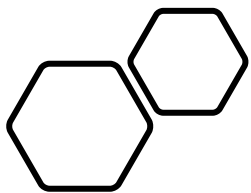
# System Design – Private UPGMA



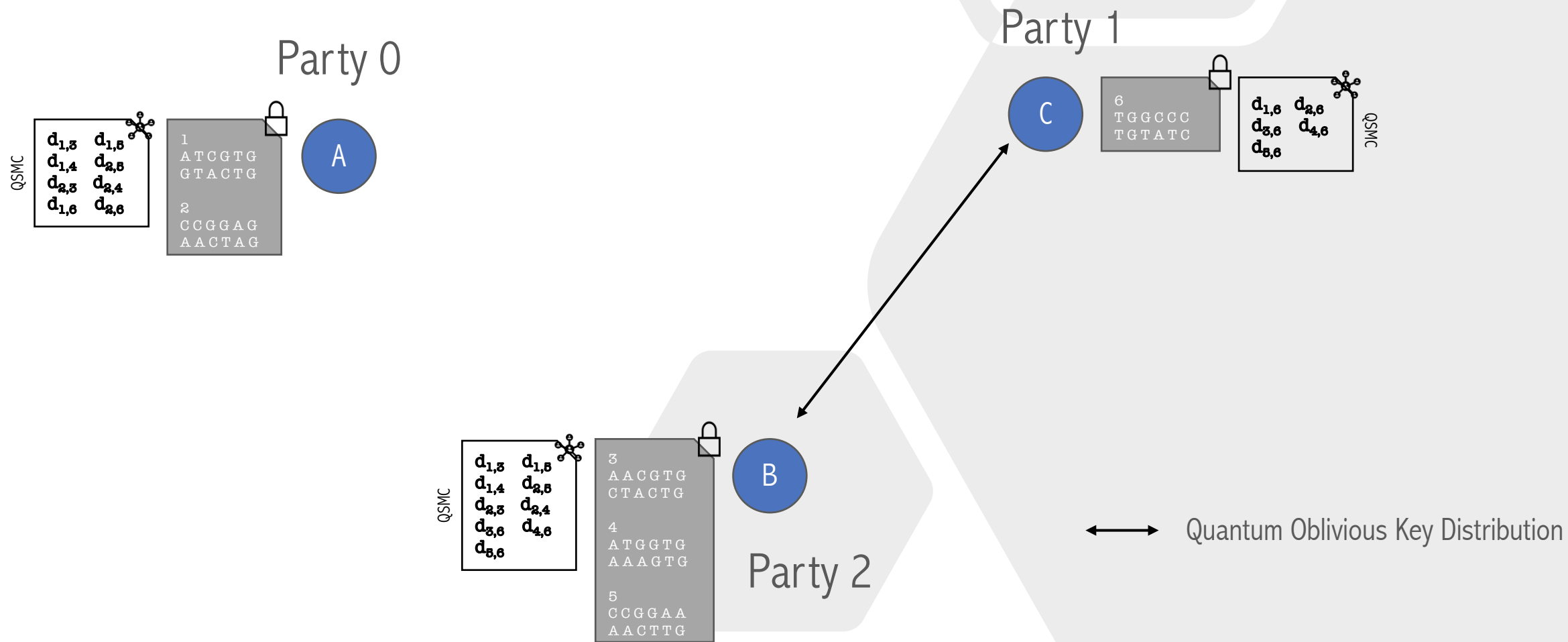


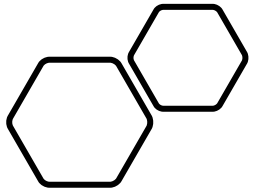
# System Design – Private UPGMA



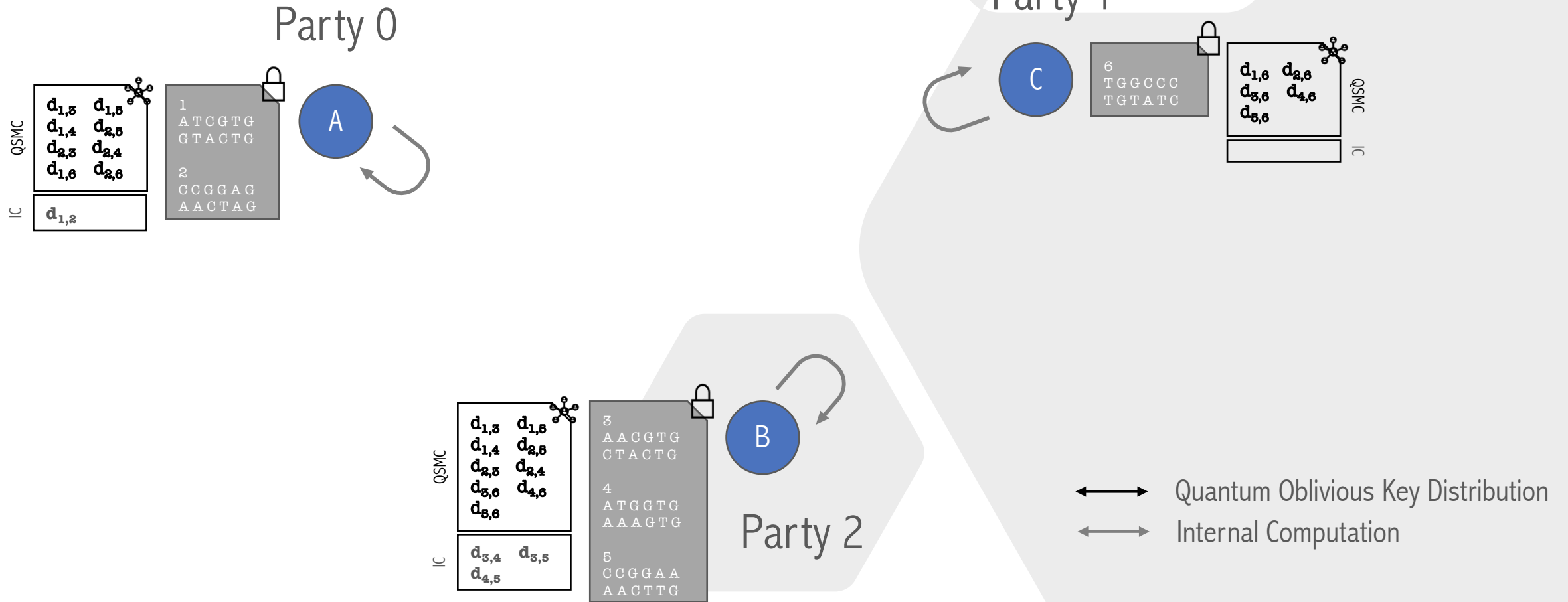


# System Design – Private UPGMA

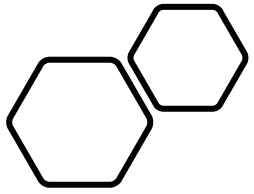




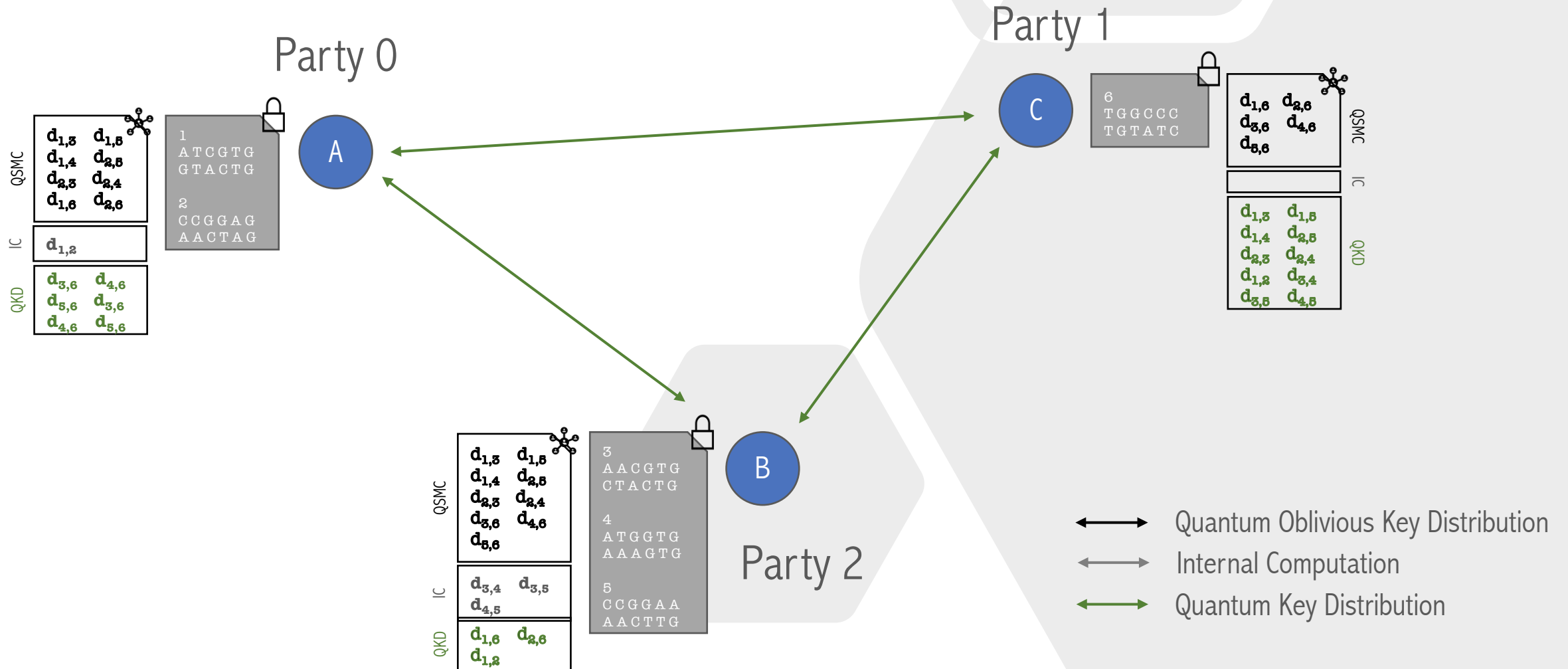
# System Design – Private UPGMA

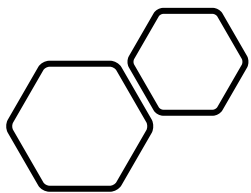






# System Design – Private UPGMA





# System Design – Private UPGMA

