Multi-party Like A BOSS: Blinded Oblivious Secret Sampling for FHE-based MPC

Organizations often need to jointly analyze their private data—for example, hospitals collaborating on a medical study—without exposing their confidential data to each other. Fully Homomorphic Encryption (FHE)-based MPC makes this possible: computations run directly on encrypted data, and only collective agreement can decrypt the results. However, conventional multi-party key generation produces secrets that grow with the number of participants. This increases noise and overhead, requiring costly workarounds as parties are added. We describe a new joint key generation procedure that produces keys whose underlying secret distribution matches the single-party setting—meaning computation proceeds as in single-party FHE regardless of party count.