What anonymity primitive is central, and how does it differ from classical overlays?

The central anonymity primitive described in the paper is quantum anonymous communication (QAC), which is compared to classical anonymous communication (CAN) . Classical overlays obscure traffic paths using multiple relays, random mixing, and encryption layers. The anonymity in CAN is achieved due to computational complexity, and vulnerable to traffic analysis or compromised relays.

QAC lets parties exchange information without revealing who sent or received it. QAC guarantees complete anonymity, untraceability, and unconditional security thanks to principles of quantum mechanics. The anonymity is built into QAC through entanglement and superposition.