# Yao’s Garbled Circuits Optimizations

This paper presents an efficient implementation of Yao's garbled circuits enhanced with several optimization techniques: point-and-permute, free XOR, row reduction (GRR3), and half gates. These techniques address key performance bottlenecks in traditional garbled circuit implementations, enabling significant reductions in communication overhead and computation time. My implementation demonstrates substantial performance improvements for secure multi-party computation.