Title: New Advances in Garbling Circuits

Yao’s garbled circuit (GC) construction is a central tool for constant-round secure computation and has several other applications. The GC transformation maps a boolean circuit $C$ into a “garbled circuit” $C'$, and an $n$-bit input $x$ into a short “garbled input” $x'$, such that $C'$ together with $x'$ reveal $C(x)$ and no additional information about $x$. Crucially, the mapping from $x$ to $x'$ is simple (e.g., affine) and the length of $x'$ does not depend on the size of the circuit. In applications, the latter property leads to low online complexity, as one can typically compute $C'$ ahead of time.

We present two new garbled circuit constructions extending the scope and improving the efficiency of known constructions.

(1) We reduce the size of the garbled input $x'$ from $n*k$ to $n+k$, where $k$ is the security parameter. This gives rise to a GC with “optimal” asymptotic rate of 1. As an application, we obtain protocols for secure multiparty computation and non-interactive verifiable computation in the preprocessing model which achieve, for the first time, an optimal online communication complexity. Based on a joint work with Yuval Ishai, Eyal Kushilevitz and Brent Waters.

(2) We show how to garble *arithmetic* circuits in which the input $x$ consists of $n$ integers from a bounded (but possibly exponential) range. This is the first extension of the GC technique to the arithmetic setting. Based on a joint work with Yuval Ishai and Eyal Kushilevitz.