Abstract:

Motivated by the goal of securely searching and updating distributed data, we introduce the notion of function secret sharing (FSS), a form of “additive secret sharing” for $f: \{0,1\}^n \rightarrow G$, where $G$ is an abelian group.

An m-party FSS scheme for function class $F$ allows one to split any function $f$ from $F$ into m succinctly described functions $f_i$, such that: (1) for every input $x$, $f(x)$ is equal to the sum of evaluations $\sum_i f_i(x)$, and (2) any strict subset of "share functions" $f_i$ hides $f$. FSS provides a natural generalization of distributed point functions, as introduced by (Gilboa-Ishai Eurocrypt 2014), which coincide with the special case of two parties and the class $F$ of point functions (which evaluate to 0 at all but one point).

We present two types of results:
- We obtain efficiency improvements and extensions of the original distributed point function construction.
- We then initiate a systematic study of general FSS, providing constructions for richer function classes, and establishing relations with other cryptographic primitives.

Joint work with Niv Gilboa and Yuval Ishai.