PETER RINDAL

(509) · 520 · 8701 ⋄ rindalp@OregonState.edu
1445 NW Vista Pl. ⋄ Corvallis, OR 97330
web.engr.OregonState.edu/~rindalp

RESEARCH STATEMENT

My main research agenda is the development of cryptographic protocols, with a focus on secure computation. The bulk of this research has been centered on the question of efficiency of secure computation. This type of computation allows a group of distrusting and possibly malicious parties to perform computation on private data, such that only the outcome of the computation is learned. Over the last several decades enormous progress has been made on general purpose techniques for performing such computations. However, there remains a significant gap between the start-of-the-art and what is require for practical applications. My research has aimed at addressing this issues by designing provably secure protocols which are targeted at specific applications.

The most notable line of research in this direction has been on the problem of Private Set Intersection (PSI). Consider a group of parties each holding a list of items. These participants wish to discover which items they have in common but not reveal any information about items unique to some of the parties. This type of functionality has many applications ranging from discovering which of your friends also use an app to securely querying whether your genes contain a life threating mutation. My research has resulted in several of the most efficient protocols for this problems across different setting.

Another very active area of my research has been into the problem of training machine learning models on private data which is distributed between several parties. As with PSI, this problem is too computationally intensive to performing using generic approaches. In a recently published work we showed that, by revealing slightly more information than the final model, even complex neural nets can be trained on large distributed datasets. Central to the efficiency of our approach is a careful application of secure computation and differential privacy, along with a detailed examination of how many machine learning methods leverage slight variations on the gradient decent algorithm.

My future research direction is to continue to improve the efficiency of secure computation using applications specific techniques. Numerous open problems remain in both the PSI and machine learning domains. In the former, combining existing techniques with additional functionality could enable new and interesting application such as more accurate national voter registration without imposing privacy concerns typically associated with voter data. Furthermore, as machine learning technique become over more popular along with mounting privacy concerns, resolving these conflicting forces in a more efficient and secure manner with be of the utmost importance.