Theme: Privacy Preserving Computing

- Sub Theme:
  - Privacy Preserving Machine Learning / Deep Learning
  - Privacy Preserving Data Analytics
  - Privacy Preserving Computing Applications

Privacy-Preserving Computing (PPC) has emerged in recent years to enable the secure computation of the data without revealing the content of the data. An example of the PPC includes the homomorphic encryption that enables operation on the encrypted data without decryption. Another example of the PPC is the multi-party computation that allows jointly computing a function over their inputs while keeping those inputs private. Unfortunately, privacy-preserving computing comes at a cost: current versions of these technologies are computationally costly, difficult to program, and hard to configure for different use cases.

We are aiming to find efficient approaches to enable privacy preserving machine learning / deep learning (PPML / PPDL) and data analytics (PPDA) using the homomorphic encryption and/or secure multi-party computation. These approaches may include researches on neural network models and efficient computations for PPML / PPDL, new data analytic algorithm and library for PPDA, programming languages and compilers for ease of use and automatic optimization, and so on. We also look for real world applications using the Privacy-Preserving Computing.

※ The topics are not limited to the above examples and the participants are encouraged to propose original idea.
※ Funding : Up to USD $150,000 per year