Theme: Homomorphic Encryption

- Sub Theme:
  - Cryptanalysis of Homomorphic Encryption
  - Comparison and Search Algorithms
  - Authentication of Homomorphic Computation Result
  - Efficient hardware acceleration of homomorphic encryption and its applications

Homomorphic encryption is the next generation cryptography based on the Ring-Learning With Errors problem (RLWE); It allows computation on the encrypted texts resulting in the new encrypted text. When the new encrypted text is decrypted, the result of the computation is the same as the result of the computation on the unencrypted text. This new cryptography enables users to store encrypted data in the cloud without revealing the content of the data to the cloud operator, and perform useful computation on the encrypted data in Cloud.

There are number of homomorphic encryption algorithms recommended for use from the Homomorphic Encryption Standardization with the list of open source libraries that implemented the algorithms. However, their software performances are painfully slow and provide limited functionality for computation. Different algorithms use different mechanisms, parameters, and bootstrapping techniques for different use cases without the clear documentation and guidance for developers.

We are aiming to analyze the security of the standardized algorithms and their implementation in the open source libraries for different use cases to ensure that they are safe to use and provide the best implementation of the recommended algorithms. Some algorithms and open source libraries allow only addition and multiplication, but do not allow comparison and search. We need the most efficient, fully parallelized, and secure implementation of the
standardized homomorphic encryption algorithms optimized for HW implementation that also support not only the addition and multiplication but also compare and search. We also look for the solution that ensures any operation on the encrypted data can be trusted when decrypted with the private key.

※ 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