Mathematical Theory Applied in Coding and Cryptography

Coding and cryptography are an essential subjects in the fields of information security and communication, and they have been applied widely in information technology for several decades of years. Coding and cryptography are closely related to many mathematical subjects, such as, algebra, number theory and combinatorics. An in-depth study of coding and cryptography needs profound methodology in such mathematical fields.

In this workshop, we will invite excellent specialists in mathematics, coding and cryptography to exchange their ideas, communicate the latest results and develop further collaborations. Topics of this workshop include but are not limited to:

(1) Open problems and conjectures in coding theory;

(2) Optimal error-correcting codes, sequences and cryptographic functions designed by using the tools of the theories of finite field, combinational design and exponential sum;

(3) Links between cryptographic functions and mathematical structures such as semi- field, permutation polynomial, difference set and hyper-elliptic curve.

(4) Algebraic geometry codes, computational number theory and the related problems.

Organizers

Name	University
Maosheng Xiong	Hong Kong University of Science and Technology
Rongquan Feng	Peking University, China
Mei Lu	Tsinghua University, China
Jing Yang	Tsinghua University, China