

XING Chaoping Professor

Division of Mathematical Sciences
School of Physical & Mathematical Sciences
PhD, University of Science and Technology of China

Major Research Interest: **Algebraic Curves, Number Theory, Coding Theory & Cryptography, Quasi-Monte Carlo**

Email: xingcp@ntu.edu.sg
Tel: (65) 6513 8170
Fax: (65) 6316 6984



Algebraic curves over finite fields have been and are still attracting number theorists and geometers since the proof of Riemann-Weil hypothesis in 1940s. Many important and fruitful results and ideas have arisen out of this area, where number theory and geometry meet. Nowadays, a new subject called arithmetic geometry has grown from this fascinating area. For a long time, study of algebraic curves over finite fields was a territory of pure mathematics. However, due to the stunning discovery of algebraic geometry codes by Goppa in 1980-1982, the theory of algebraic curves over finite fields has attracted new groups of researchers such as coding theorists, cryptographers and algorithmically inclined mathematicians. In the last two decades, several other interesting applications of algebraic curves over finite fields, including the elliptic curve based cryptosystems, low-discrepancy sequences and combinatorial cryptography, have been found.

Our research includes the following:

Curves with many rational points

There have been tremendous research activities focused on algebraic curves over finite fields with many rational points in the last ten years due to more and more applications. Constructing algebraic curves with many points has been the major task for this subject. The main tools employed in this topic are from number theory and algebraic geometry.

Constructions of codes from number theory and algebraic geometry

A breakthrough in coding theory was the introduction of algebraic geometry to construction of good block codes. In the last ten years, algebraic geometry (in particular algebraic curves over finite fields) has been extensively used by us to obtain various constructions of good block codes. Recently, we have successfully applied number theory and algebraic curves to constructions of quantum codes and space-time codes.

Constructions of cryptographic schemes from algebraic geometry

Nowadays, algebraic geometry has found a widespread application in cryptography. Apart from the well-known elliptic curve cryptosystem, algebraic geometry has been applied to constructions of many schemes in cryptography such as hash functions, frameproof codes, secret sharing, key exchange, etc. One of our goals in this area is to find more application of algebraic geometry in cryptography.

Constructions of low-discrepancy sequences from algebraic curves.

Low-discrepancy sequences play a key role for quasi-Monte Carlo method which is a deterministic version of Monte Carlo method. Constructing quasi-random points is a challenging problem in this topic. We have applied algebraic curves with many rational points to construction of Low-discrepancy sequences and we are still looking for some further tools from number theory to construct quasi-random points.

Selected Publications

K. Q. Feng & C. P. Xing, A new construction of quantum error-correcting codes, *Trans. of the AMS*, **to appear**.

C. P. Xing & S. L. Yeo, Algebraic curves with many points over the binary field, *Journal of Algebra*, **311** (2007) 775–780

C. P. Xing, Nonlinear codes from algebraic curves improving the Tsfasman-Vladut-Zink bound, *IEEE Trans. on Information Theory*, **49**(2003) 1653-1657.

A. Garcia, H. Stichtenoth & C. P. Xing, On subfields of the Hermitian function fields, *Compositio Mathematica*, **120** (2): (2000) 137-170.

H. Niederreiter & C. P. Xing, Quasirandom points and global function fields, *Finite Fields and Applications* (S. D. Cohen and H. Niederreiter, eds.), London Math. Soc. Lecture Note Series 233, 269-296, Cambridge University Press, Cambridge, 1996. **Featured Review (97j:11037)**