I am interested in analyzing and improving the security of communication and computer systems. I am working on the design and attack of symmetric key ciphers; and I am interested in analyzing the security of computer software.

CRYPTOGRAPHY
To protect the confidentiality and integrity of information, ciphers have been widely used in military, intelligence and diplomatic services. Today cryptography plays an important role in daily life to protect mobile phones, emails, electronic access cards, bank transactions, electronic passports...

Cryptography is to design ciphers to resist various attacks. Cipher designers need to know all the existing attacks very well, and to have the intuition of future attacks. Cipher designers need to develop elegant approaches to resist attacks, so that the security of a cipher can be evaluated relatively easily.

I am working on the design of symmetric key ciphers to achieve strong security and high performance. I have designed stream cipher HC and hash function JH. Stream cipher HC-128 achieves the encryption speed of about 3 clock cycles/byte on a normal desktop computer, and it is a winner of eSTREAM, the stream cipher project of the European Network of Excellence for Cryptology (2004–2008). Hash function JH is a finalist of the NIST hash function competition (2008–2012).

CRYPTANALYSIS
Cryptanalysis is to analyze the security of a cipher. It is the foundation of cryptology research. I mainly work on the cryptanalysis of symmetric cryptographic algorithms, including block ciphers, stream ciphers, message authentication codes and hash functions. Block ciphers and stream ciphers are used for symmetric key encryption; message authentication codes are used for protecting the integrity of messages; hash functions are used for generating message digests for digital signatures. I have broken more than twenty ciphers, including breaking the recent ZUC cipher (in 2010) used in the preliminary 3G security standards 128-EEA3 and 128-EIA3.

COMPUTER SECURITY
Today personal computers and smart phones are widely used to access and process confidential information. Computer security deals with the flaws in the design and implementation of computer systems. It is a big challenge to ensure that a computer system is secure since computer system is complicated in general.

I am interested in exploiting security flaws in computer software. Software is the basic component of operating system and many applications. Finding software flaws is important for improving the security of computer system.