## 学术报告

**Title:** **Standardising cryptography – a personal view**

**Speaker:** **Dr. Liqun Chen**
(*principal research scientist at Hewlett-Packard Laboratories in Bristol, UK*)

**Time:** 2015年9月16日（周三） 下午3：00

**Venue:** 清华大学 高等研究院（科学馆）322 报告厅

## Abstract

If you designed a cryptographic scheme and published it in a well reputed journal or presented it at a prestigious conference, the life of this scheme has only just begun. If you want the scheme to be used there are still many hurdles to overcome; the road to acceptance is a long one. There is an enormous distance between a theoretically well founded cryptographic scheme and a practical cryptographic solution. Standardisation is a vitally important bridge between theory and practice and getting your scheme included in a relevant standard is your chance to get your crypto design widely used. In this talk, we discuss why standardisation is important and how cryptographic schemes are standardised.

报告人简介：Dr. Liqun Chen is a principal research scientist at Hewlett-Packard Laboratories in Bristol, UK. She is known for her work in both the cryptographic and trusted computing communities. She designed some of the cryptographic algorithms used in the Trusted Platform Module (TPM) of Trusted Computing Group (TCG); based on information from the TCG, at least 500 million TPMs have been shipped. She has also developed several cryptographic schemes adopted by International Standards, and has served as editor, or co-editor, for five ISO/IEC standard documents. Liqun has an extensive publication record and holds 56 granted US patents in cryptography and information security. Her co-authored paper originally published at ACM CCS 2004 was given a test of time award at ACM CCS 2014. Liqun obtained her BSc, MSc and PhD in Engineering from Southeast University in P. R. China. Prior to joining HP, she worked at Southeast University, the University of Oxford and Royal Holloway, University of London.