# 清华大学高等研究院

Institute for Advanced Study, Tsinghua University

## 密码学学术报告 Cryptology Seminars

**Title:** **Structural Lattice Reduction: Generalized Worst-Case to Average-Case Reductions**

**Speaker:** **Prof. Phong Q. Nguyen**
（法国国家信息与自动化研究所主任、清华大学高等研究院访问学者）

**Time:** **4:00pm, Monday, May 20, 2013** **(3:30~4:00pm, Tea, Coffee, and Cookie)**

**Venue:** **Conference Hall 322, Science Building, Tsinghua University**

## Abstract

There is growing interest in lattice-based cryptography, reinforced by the recent discovery of fully-homomorphic encryption and noisy multi-linear maps. A central question in lattice-based cryptography asks which family of lattices are suitable for cryptographic applications. Over the years, many different families of lattices have been proposed, both in theory and in practice, but it is still unclear which family offers the best security/efficiency trade-off. From a complexity point of view, the most interesting family is the one proposed by Ajtai at STOC '96, when he presented the first worst-case to average-case reductions for lattice problems: if one can find very short vectors in Ajtai's random lattices, then one can efficiently find short vectors in any lattice. Since 1996, worst-case to average-case reductions have been significantly improved, but the average-case problem has essentially not changed: it refers to a very special class of lattices related to the group G=(Z/qZ)^n. We generalize worst-case to average-case reductions for lattice problems(namely, Ajtai's SIS and Regev's Search-LWE) to almost all integer lattices, by allowing to replace the group G by any (sufficiently large) finite abelian group. By taking G=Z/pZ for large prime p, we obtain the first hardness results for the lattices used in the main lattice reduction benchmarks and in Darmstadt's SVP challenges, and for the hidden number problem introduced by Boneh and Venkatesan to study the bit-security of Diffie-Hellman key exchange. And by taking G as a cyclic group, we obtain that most integer lattices are as hard as worst-case lattices. Our main tool is a novel group generalization of lattice reduction, which we call structural lattice reduction, and which might be of independent interest.

This is joint work with Nicolas Gama (UVSQ, France) and Malika Izabachene (LORIA, France)

Phong Q. Nguyen 于1994和1996年分别取得里昂高等师范学校计算机科学专业学士和硕士学位，1999年获得巴黎高师和巴黎第七大学博士学位。2000年至2008年在法国国家科学研究中心研究员，2007年获得巴黎第七大学和巴黎高师教授资格，2008年至今担任法国国家信息与自动化研究所主任。主要从事密码分析和算法数论的研究，共发表了50多篇国际会议论文。2001年获得了ERCIM的Cor Baayen 奖。2006年获得了欧密会最佳论文奖。自2006年起担任密码期刊Journal of Cryptology 和 Journal of Mathematical Cryptology副主编。30多次作为国际密码会议程序委员会成员，包括密码领域权威的三大会议美密会（CRYPTO）、欧密会（EUROCRYPT）和亚密会（ASIACRYPT），并作为EUROCRYPT 2013/2014、PKC-2012的程序委员会联合主席。