

**On some easy and not-so-easy
problems**

Dr. Vassil Simeonev Dimitrov
Research Fellow
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University



Date : 27 March 2009 (Friday)
Time : 5.30 pm – 6.30 pm
Venue: SPMS-Seminar Room, MAS-03-08
School of Physical and Mathematical Sciences

Multiplication of two integers is a problem that has been almost exhaustively analyzed by computer scientists and mathematicians. In the 50-ies, Kolmogoroff made a conjecture that any multiplication algorithm should have a quadratic complexity. The discovery of Karatsuba multiplication in 1963 disproved this conjecture in a rather simple manner. However, there are still unknown features associated with this simple computational problem, even in the case when one of the multiplicands is unknown. Since modern public key cryptography uses very large multipliers, it seems important to know certain nontrivial upper bounds. For example, given any 150-bit integer, x , how many additions are sufficient to implement multiplication by x if one uses binary additions and shifts only? What would be the role of the subtractions? What are the worst cases? In this talk we shall try to address some of these issues and point out various potential applications.

Host: Coding and Cryptography Research Group, Division of Mathematical Sciences,
School of Physical and Mathematical Sciences

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

NANYANG TECHNOLOGICAL UNIVERSITY
SPMS-MAS-03-01, 21 NANYANG LINK, SINGAPORE 637371
FAX: +65 6515 8213 TEL: +65 6513 7423