



The University of Western Ontario

Faculty of Science

Department of Applied Mathematics

APPLIED MATHEMATICS COLLOQUIUM

Date: Wednesday, May 28, 2008

Time: 2:30 pm

Location: Middlesex College Room 204

Three Quantum Leaps in the Developments of Encryption Algorithms

Dr. Per Kaijser
Munich, Germany

Abstract:

This paper gives a coarse overview of the historical development of algorithms used for information security. It is shown that the development of these encryption algorithms has been made in small incremental steps for almost 2000 years until the latter part of the last century, when three revolutionary inventions were made. The main properties of these technologies, the public key encryption method, quantum cryptography and quantum computing are explained and it is demonstrated why these can be seen as quantum leaps in this development.