2021 Conference on Retirement of Prof. Yeong-Nan Yeh
Institute of Mathematics, Academia Sinica, Taipei, Taiwan
June 27-28, 2021

On Postquantum Cryptography

Bo-Yin Yang
Academia Sinica
byyang@iis.sinica.edu.tw

Abstract

Quantum Computers (using Shor's Algorithm) can break all currently deployed public-key cryptography. Therefore we need to migrate to public-key cryptosystems that can resist quantum computing. These cryptosystems are called Postquantum, and the study of such systems Postquantum Cryptography (PQC). I will tell you the recent story of PQCs and discuss some mathematics dealing with PQC.