-- 横山俊一（首都大学東京）--

Magma [1] (distributed at the U. Sydney) is a software designed for computations in algebra, number theory, and arithmetic geometry.
In this talk, we will introduce Magma and extensive projects with packages we created (or collaborated) with short demos.
If time permits, we will discuss CAS for new programming language, especially Julia (NemoCAS project [2]).

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, Journal of Symbolic Computation 24 (1997) no.3–4, pp.235– 265, Computational algebra and number theory (London, 1993).

[2] C. Fieker, W. Hart, T. Hofmann and F. Johansson, Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language, Proceedings of ISSAC '17, pp.157–164.

-- Mehdi Tibouchi (NTT Secure Platform Laboratories) --

Candidates for lattice-based signature schemes in the NIST postquantum standardization process have mostly avoided discrete Gaussian distributions (preferring uniform noise instead), despite the better theoretical behavior of Gaussians and the better parameters they allow. This is mostly due to concerns regarding the difficulty of implementing noise sampling and rejection sampling securely when using Gaussians.

In this talk, we discuss previous attacks on insecure implementations of Gaussian-based signature schemes, and describe new techniques to overcome these challenges.

-- 山口純平（富士通研究所）--

The security of cryptography is based on the hardness of mathematical problems, and it is evaluated by computing the limit of solving these problems using computers.
At present, quantum computers have begun to put to practical use, such as small-scale quantum annealing computers has been developed,
it is important to evaluate the hardness of solving mathematical problems by using quantum computers.
Recently, digital computers specialized for annealing computation inspired by quantum annealing have been realized on large-scale,
which enables us to evaluate the hardness and to estimate its thread prior to the quantum annealing computers.
In this talk, I introduce how to solve two kind of post-quantum cryptographic problems(lattice problems and MQ problems) using annealing computers and
the experimental results of solving these problems by using Digital Annealer, a digital annealing computer developed by Fujitsu.