FMfl2023 Program	
Name	Yusuke Aikawa
Affiliation	The University of Tokyo
Title	**Expander Families for Post-Quantum Cryptography**
Abstract	The security of public key cryptography is supported by computational hardness of problems derived from mathematics. For example, the integer factoring problem is a basis for the security of RSA cryptography. However, in 1994, Shor proposed an efficient quantum algorithm solving these problems, for example factoring and discrete logarithm problem (DLP). This means that emergence of large-scale quantum computers will break public key cryptography in use today. So, we need cryptography that are resistant to cryptanalysis by quantum computers. Such cryptographic primitives are called post-quantum cryptography, PQC for short. In order to construct PQC, it is necessary to introduce mathematical computational assumptions that are different from factoring and DLP. In this talk, the speaker will talk about constructing a candidate of PQC from random walks on expander graphs, including our recent results. In particular, isogeny graphs of abelian varieties and Cayley graph expanders will be discussed.