Pre- and post-quantum Diffie–Hellman protocols

Benjamin Smith
INRIA, France

Abstract. This would basically be about trying to come up with a coherent framework in which classic finite field DH, ECDH, ordinary isogeny DH, and and supersingular isogeny DH are all clear instances of the same phenomenon, and then using that to - consider the hardness of the underlying DHPs, and relate them to other cryptographic problems, - including analogues of the hidden number problem; - look at when each of these protocols can be used safely for non-interactive key agreement; and - look at how they can be turned into KEMs (e.g. SIKE).