Sur les protocoles Diffie-Hellman pré- et post-quantique

Benjamin Smith*[1]

[1]INRIA, Laboratoire d'informatique de l'École polytechnique (LIX), Palaiseau – Centre National de la Recherche Scientifique : UMR7161, Ecole Polytechnique – France

Résumé

For over 40 years now, Diffie–Hellman key exchange has been a fundamental tool in public-key cryptography. This cryptosystem allows two parties to establish a shared secret value over an insecure public channel; it is the first step in setting up secure internet connections, and a building block for more complicated public-key cryptosystems. The security of Diffie–Hellman essentially depends on the computational hardness of the classic discrete logarithm problem; but while discrete logarithms may be spectacularly hard to compute with classical computers, they can be solved in polynomial time using Shor's quantum algorithm. Faced with the projected rise of powerful quantum computers, the race is on to find efficient "post-quantum" replacements for Diffie–Hellman, and other algorithms based on discrete logarithms and integer factorization, that resist known classical and quantum attacks. This talk will describe one attempt to develop a practical post-quantum drop-in replacement for Diffie–Hellman key exchange, comparing and contrasting with historic and contemporary algorithms. The key is to move from discrete logarithms, which represent relationships between points on elliptic curves (the heart of the current state-of-the-art in Diffie–Hellman), to isogenies, which represent relationships between elliptic curves themselves. (We will maintain a somewhat high-level perspective on the subject, avoiding most of the gory algebraic geometry.)

*Intervenant