Spring 2017

Nonabelian Group Based Cryptography

Timothy (Tim) Huber
Washington University in St. Louis

Nonabelian Group Based Cryptography

Timothy (Tim) Huber

Mentor: John Shareshian

Concerns over the security of RSA public-key cryptography with the potential development of quantum computers renewed interest in novel cryptosystems that do not rely on commutative groups. We provide an introduction to public-key cryptography along with an explanation of the AAG and Ko-Lee key agreement protocols with their originally proposed platform group, the braid group. We will then discuss two successful attacks against the AAG cryptosystem with consideration for practical concerns and known empirical results.