Mathematics of Post-Quantum Cryptography

Algebraic Cryptography Center at Stevens Institute of Technology

---

Robert Gilman

(Stevens Institute of Technology)

The search for hard problems

Abstract:

The security of a public key cryptosystem usually depends on an associated computational problem, which should be difficult to solve almost all the time for an appropriate choice of parameters. There are a number of existence proofs, but there do not seem to be any concrete examples of problems which are provably hard to solve almost all the time. We review the situation and make some suggestions about where one might look. Contributions from the audience are welcome.