Physical Attacks Against Lattice Based Cryptography

Philip Hodgers, Richard Gilmore, Ciara Moore, Markku Saarinen, Maire O'Neill, Tobias Oder, Tim Guneysu, Felipe Valencia, Francesco Regazzoni

Abstract

Lattice-based cryptography is a promising replacement for existing public-key systems, since it is believed to be resistant against quantum attacks and has a relatively limited key size. Current research efforts in the field are mainly concentrated on designing efficient cryptosystems and implementing them in a efficient way, leaving the problem of their resistance against physical attacks largely unexplored. In this talk we report potential weaknesses which might affect physical implementations of lattice based cryptosystems, we summarize current research on countermeasures, and we highlight potential future research directions.