Title:
Secret key extraction by BIKE flipping

Author:
Tarick Welling

Abstract:
Quantum Computers are a major threat to current cryptography. To combat this new threat BIKE has been proposed as a replacement. Conventional threats such as physical attacks remain relevant to these new crypto and need to be investigated. We set out to extract the secret key by means of flipping the BIKE-Flip decoder and use Side Channel Analysis for extraction.