Tomáš Fabšič

The threat of quantum computers for cryptography

Abstract

It is known that large quantum computers will be able to break all asymmetric cryptosystems which are in common use today. Although no large quantum computers currently exist, significant progress is being made in their development. In this talk, I will discuss how imminent the threat of quantum computers is, and what steps the cryptographic community currently undertakes to prepare for this threat.