# Zamyšlení nad post-kvantovou kryptografií

## David Pikálek (KPMG)

Kryptografie je dnes přítomna jako základ moderní civilizace. Kryptografické algoritmy jsou zabudované do běžných zařízení spotřební elektroniky a spoléháme na ně v každodenním životě. Současné algoritmy se vyvíjely cca 100 let a stojí na ještě starších matematických základech. S rozvojem poznání fyziky se začínají do praxe prosazovat kvantové počítače, které provádějí operace nikoliv jako logické nebo číselné výpočty v binárním kódu, ale na základě kvantových jevů. Spolu s nimi ale přichází ohrožení pro bezpečnost používaných kryptografických algoritmů.

V přednášce si vysvětlíme, co se označuje jako klasická, kvantová a post-kvantová kryptografie. Shrneme připravované algoritmy post-kvantové kryptografie, jaký je stav jejich standardizace a očekávaný postup přijetí do praxe. Vysvětlíme si možné budoucí hrozby kvantových počítačů vůči kybernetické bezpečnosti. Uvidíme, proč a jak se již dnes připravovat na post-kvantovou kryptografii i v provozu informačních systémů.

*David vystudoval Teoretickou kybernetiku, informatiku a teorii systémů na MFF UK. Má více než 30 let zkušeností v oboru informačních technologií. Jako konzultant KPMG se specializuje na implementace systémů řízení kybernetické bezpečnost, a to zejména v prostředí kritické informační infrastruktury státu.*

**středa 24. dubna**

**17:30 v posluchárně K1**

MFF UK, Sokolovská 49/83

nebo live stream na YouTube

MATEMATICKÉ PROBLÉMY NEMATEMATIKŮ

www.karlin.mff.cuni.cz/mffseminar najdete nás i na FB