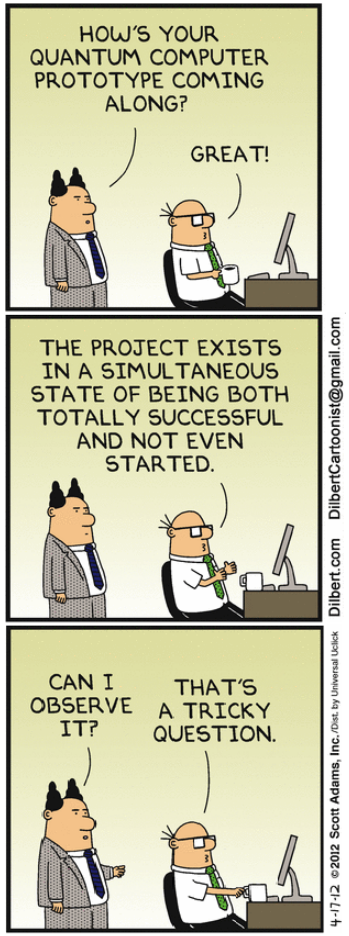
Kvantový počítač – pátý jezdec apokalypsy?

Ing. Tomáš Rosa, Ph.D. (Raiffeisenbank)



Začalo to snahou o efektivní simulaci chování hmoty na molekulární úrovni a níže. Nakonec, toto je dodnes jedno z hlavních témat pro kvantové počítače, tedy výpočetní stroje založené na principech kvantové mechaniky. Pak se však ukázalo, že kvantové platformy také schůdně zvládnou řešení těch matematických úloh, o jejichž obtížnost je dnes opřena naprostá většina kryptografických protokolů. Od té doby je kvantový počítač automaticky spojován s představou bezpečnostní apokalypsy.
Na přednášce se teoreticky i prakticky podíváme, odkud se ona algoritmická síla bere a jakým způsobem může posunout hranice praktické kryptoanalýzy. Budeme se přitom věnovat i na první pohled okrajovým, a tedy poněkud přehlíženým algoritmům a přístupům, které však v konečném důsledku mohou do ochrany informací rovněž silně promluvit, a to navíc podstatně dříve, než je běžně očekáváno.

Tomáš Rosa vystudoval na FEL ČVUT v kombinaci s MFF UK v Praze, doktorát získal v oboru kryptologie s cenou rektora ČVUT. Věnuje se matematicko-fyzikálním metodám počítačové a rádiové bezpečnosti. Jeho práce pomohla zlepšit několik celosvětových standardů, konkrétně protokol TLS, platební schéma EMV, bezdrátový standard Bluetooth a radionavigační systémy GNSS. Je hlavním kryptologem kompetenčního centra skupiny Raiffeisen Bank International.

středa 20. listopadu

17:30 v posluchárně T-201

FJFI ČVUT, Trojanova 13

Na TUL se živý stream přednášky koná od 17.30 hodin v posluchárně G313!!

MATEMATICKÉ PROBLÉMY NEMATEMATIKŮ

www.seminar.fjfi.cvut.cz najdete nás i na FB a YouTube