POZVÁNKA na 36. setkání PRAŽSKÉHO INFORMATICKÉHO SEMINÁŘE

HARRY BUHRMAN

Kvantový software a jeho využití pro poziční kryptografii

po přednášce bude následovat diskuse

24. května 2018
16 hod.

Posluchárna S5, MFF UK
Malostranské nám. 25,
Praha 1

ANOTACE PŘEDNÁŠKY

Kvantové počítače skýtají velký příslib pro hardware nové generace. Jsou založeny na překvapivých jevech z kvantové mechaniky, jako jsou superpozice, interference nebo provázanost stavů. Základním stavebním kamenem kvantového počítače je kvantový bit, tzv. qubit, který na rozdíl od klasického bitu může být v kvantové superpozici, tj. v jakési kombinaci nuly a jedničky. V devadesátých letech bylo prokázáno, že pro specifické problémy mohou kvantové algoritmy běžící na kvantovém počítači výrazně překonat klasické počítače. Slavný kvantový algoritmus Petera Shora ukazuje, že kvantový počítač může faktorizovat velká čísla a tím prolomit většinu současné kryptografie. V posledních letech došlo k významnému pokroku ve vývoji hardwaru pro kvantový počítač. Společnost IBM vyvinula zařízení s 50 qubity a Google nedávno oznámil vytvoření zařízení se 72 qubity. S touto rychlostí růstu budeme mít během pěti let 100 qubitů, a velké kvantové počítače lze tedy očekávat během 5-10 let. Co lze počítat na kvantovém počítači, a jak může být užitečný? V této přednášce podáme krátký úvod do kvantového počítání a software, a ukážeme jeho využití pro kryptografii založenou na pozici.

Dne 20. července 1969 miliony lidí zatajily dech, když sledovaly živé televizní vysílání, při kterém Neil Armstrong vystoupil na Měsíc. Přesto televizní stanice Fox uvádí, že ohromujících 20% Američanů o misi Apollo 11 pochybuje. Mohla to být podvodná inscenace natočená v hollywoodských studiích na Zemi? Poziční kryptografie může nabídnout řešení pro takové problémy. Tento druh kryptografie používá geografickou polohu účastníků jako jediné pověření namísto digitálních klíčů nebo biometrických prvků.

O PRAŽSKÉM INFORMATICKÉM SEMINÁŘI

Seminář se schází vždy 4. čtvrtek v měsíci v 16 hod. (s výjimkou letních měsíců a prosince), a to buď v budově FEL ČVUT na Karlově náměstí, nebo v budově MFF UK na Malostranském náměstí. Jeho program je tvořen hodinovou přednáškou, po níž následuje časově neomezená diskuse. Základem přednášky by mělo být něco (v mezinárodním měřítku) mimořádného nebo aspoň pozoruhodného, na co přednášející přišel a co vysvětlí způsobem srozumitelným a zajímavým i pro širší informatickou obec. Přednášky jsou standardně v angličtině.

Harry Buhrman je profesorem algoritmů, teorie složitosti a kvantového počítání na Amsterdamské univerzitě (UvA), vedoucím skupiny kvantového počítání v Ústavu pro matematiku a informatiku (CWI) a výkonným ředitelem výzkumného centra QuSoft pro kvantový software, které spoluzaložil v roce 2015. Vybudoval kvantovou výpočetní skupinu na CWI, která byla jednou z prvních skupin na světě a první v Nizozemsku. Buhrmanův výzkum se zaměřuje na kvantové výpočty, algoritmy a teorii složitosti. Je spoluzakladatelem oblasti kvantové komunikační složitosti pro distribuované výpočty, kde ukázal, že určité komunikační úlohy lze vyřešit exponenciálně efektivněji s použitím kvantové mechaniky. Ukázal tak, že kvantové počítače mohou urychlit nejen výpočty, ale i komunikaci. To otevřelo zcela novou oblast kvantového zpracování informace. Buhrman spoluvytvořil obecnou metodu pro stanovení limitů kvantových počítačů a rámec pro studium dotazovací složitosti kvantových algoritmů, což je látka, kterou dnes najdeme v učebnicích. Získal prestižní ocenění Vici a koordinoval několik národních a mezinárodních projektů v oblasti kvantové výpočetní techniky. Je členem vědeckých rad evropských projektů QUTE-EUROPE a QUIE2T a kanadských projektů CIFAR, IQC a INTRIQUE. Založil QIP, hlavní mezinárodní konferenci o zpracování kvantové informace, a předsedal jejímu řídícímu výboru. Mezi jeho současné výzkumné zájmy patří kvantové počítání, kvantová teorie informace, kvantová kryptografie, výpočetní složitost, Kolmogorovská složitost, distribuované výpočty, výpočetní teorie učení a výpočetní biologie.

GRAFICKÁ A MULTIMEDIÁLNÍ LABORATOŘ

Kontakt: info@praguecomputerscience.cz
Informace: www.praguecomputerscience.cz