

Kvantový počítač prolomí RSA klíč za 10 sekund, nejvýkonnějšímu superpočítači světa by to trvalo milióny let!

17.6.2023 - | Vysoká škola báňská - Technická univerzita Ostrava

Může být mnohem rychlejší než klasické počítání, což má potenciál zásadně změnit svět informačních technologií. Je tomu skutečně tak a otevírá se před námi doba kvantová?

O tom jsme si povídali s Markem Lampartem, působícím v IT4Innovations a na Fakultě elektrotechniky a informatiky, který se kvantovým počítáním zabývá.

Co je kvantové počítání?

Kvantové počítání je skutečně vysoce specifická forma počítání. Přesněji, je to oblast výpočetních věd zaměřených na vývoj technologií založených na principech kvantové teorie. Kvantové výpočty využívají jedinečné chování kvantové fyziky k řešení problémů, které jsou pro klasické výpočty příliš složité, nebo dokonce v reálném čase neřešitelné.

Jaký je rozdíl mezi bitem a kvantovým bitem, qubitem, základní jednotkou v kvantovém počítání?

Na rozdíl od klasického bitu může qubit existovat v superpozici svých dvou základních stavů, nuly a jedničky, což volně znamená, že je v obou stavech současně. Představme si situaci, kdy hodíme mincí. Klasický přístupem dostaneme hodnotu „panna“ nebo „orel“, kvantově ale získáme pravděpodobnosti, s jakou daný jev nastane. Při měření qubitu je výsledkem pravděpodobnostní výstup klasického bitu.

Jak funguje kvantový počítač?

V kvantovém počítači mohou být qubity propojeny a vytvářet tak kvantové registry, které umožňují provádět operace na větších množstvích dat současně. Kvantový počítač je postaven na principech kvantové mechaniky, jako jsou superpozice a provázanost (tzv. entanglement), což mu umožňuje pracovat s mnohem větším množstvím informací najednou, než je tomu u superpočítačů.

Jak bude vypadat kvantový počítač v IT4Innovations?

V současné době je vyvíjeno několik technologií. Nejvíce rozvinutou je technologie postavená na supravodivých materiálech, a taky se velice rozvíjí technologie tzv. iontů v pasti. V IT4Innovations bude instalována ta první technologie, a to díky projektu LUMI-Q. Supravodivostní kvantový počítač si můžeme představit jako tři velké skříně. První je lednička – tady se chladí na 14 milikelvinů a je zde uložen kvantový čip. Ve druhé skříně je kompresor, který zajišťuje chlazení. A konečně ve třetí je elektronika, která celé zařízení ovládá, provádí instrukce a také měření výpočtu. Je ovšem nutno říci, že se bude jednat o tzv. hybridní systém, který je provázán se superpočítačem, který jej de facto ovládá – předzpracovává a následně zpracovává data, která z kvantového počítače obdrží, ale taky optimalizuje samotný kvantový obvod.

V čem jsou kvantové počítače lepší než ty klasické?

Jsou známy kvantové algoritmy, které umožní modelovat molekuly a navrhovat nové materiály či léky. Klasicky jsou tyto výpočty extrémně časově náročné. Taký je znám kvantový algoritmus k faktorizaci čísel, který vymyslel Peter Shor počátkem 90. let. Tento algoritmus umožní pomocí 5 000 logických qubitů prolomit libovolný RSA klíč, a to během deseti sekund. Prolomit takovýto klíč by nejvýkonnějšímu superpočítači světa trvalo miliony let! Kvantové počítání přináší skutečný posun u velkých úloh, kde dochází k exponenciálnímu zrychlení.

Můžeme si kvantové počítání sami vyzkoušet?

Ano, v současné době si může každý zdarma spustit vlastní kvantový algoritmus pomocí cloudové služby od IBM – Qiskit. K dispozici jsou ale i jiní výrobci a máme slíbeno, že v dohledné době bude veřejnosti rovněž zpřístupněn kvantový počítač IQM či AQT. Většina rámců je postavena na programovacím jazyku Python, tedy uživatelsky velice příjemná a také je pro uživatele připravena docela slušná podpora k implementaci vlastních kódů.

Jaký osud čeká klasické počítače?

Kvantové počítače sice s největší pravděpodobností zcela nenahradí klasické počítače, ale kvantová technologie se docela určitě stane zásadním technologickým pokrokem, ba přímo skokem.

<https://www.vsb.cz/magazin/cs/detail-novinky?reportId=45587>