

NÚKIB




Národní úřad  
pro kybernetickou  
a informační  
bezpečnost

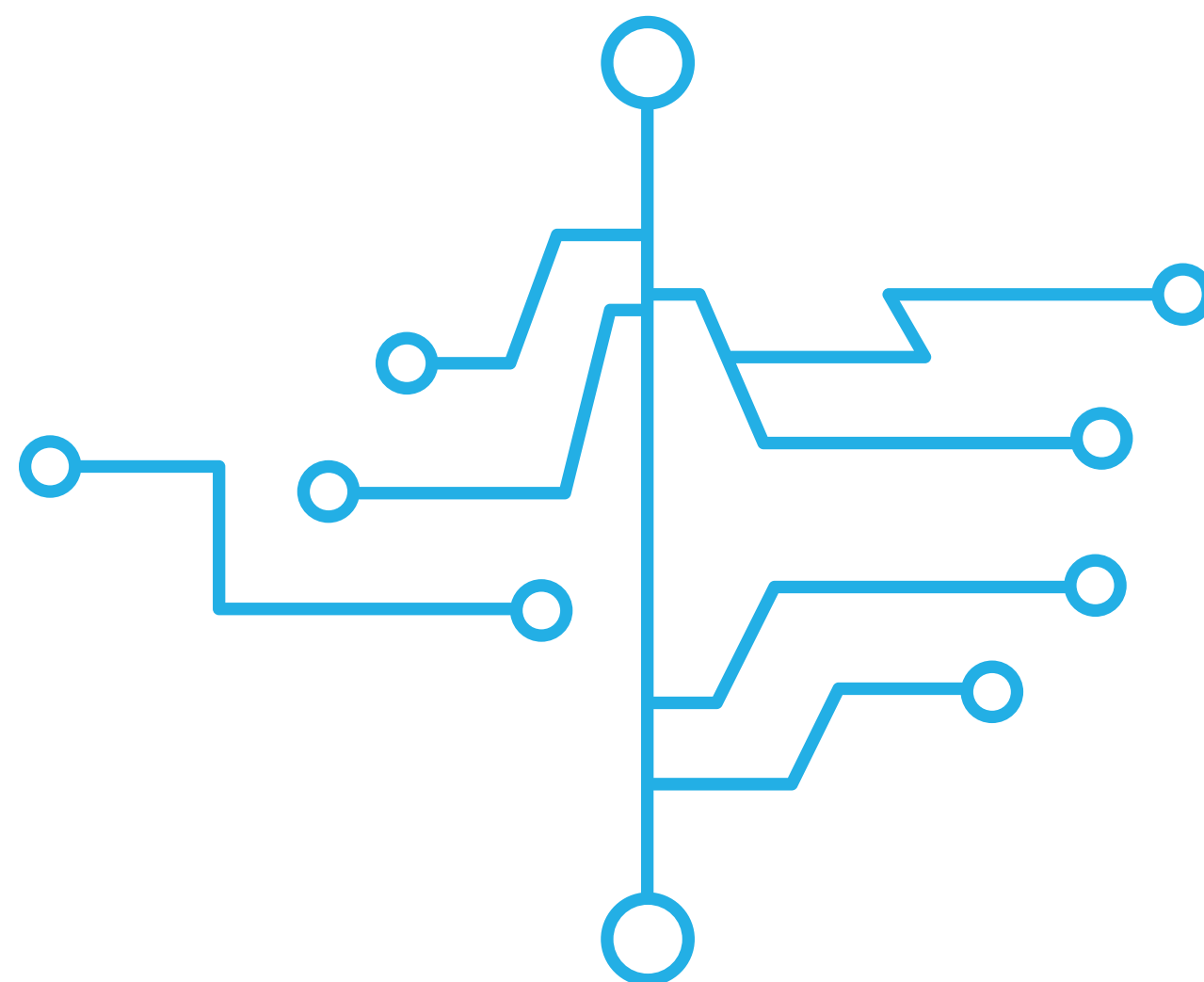
## Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

01/2024


LEDEN

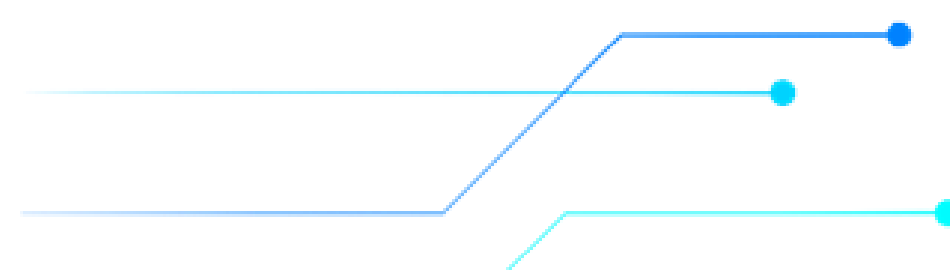
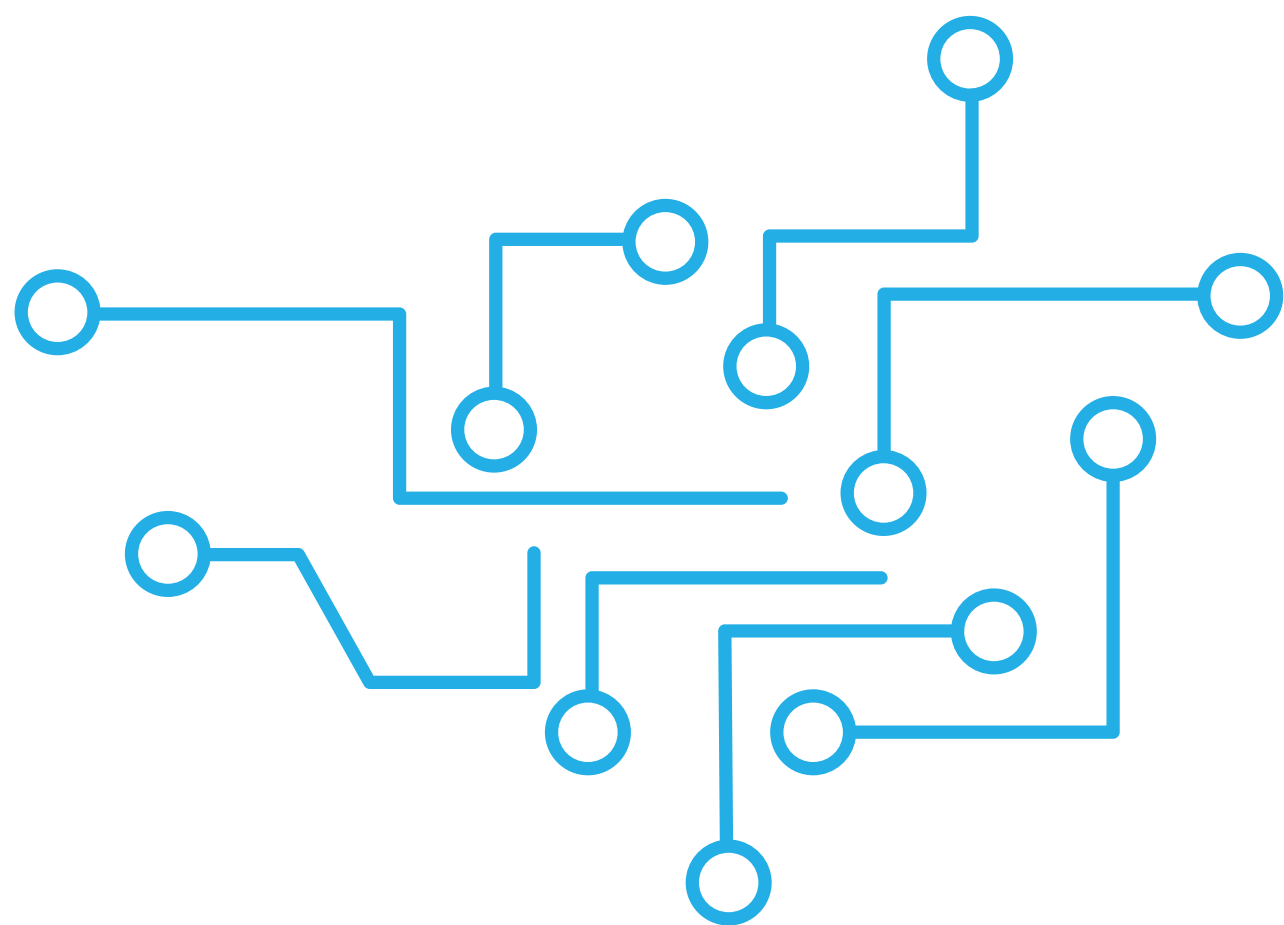
## ČVUT se jako první česká univerzita připojila do kvantové sítě IBM

České vysoké učení technické (ČVUT) se připojilo k síti IBM Quantum, jejímž prostřednictvím americká společnost IBM poskytuje vzdálený cloudový přístup ke svým kvantovým počítačům. Díky tomu je univerzita nemusí nákladně pořizovat a sama provozovat. ČVUT a IBM podepsaly memorandum o spolupráci i s dalšími českými univerzitami, které by se do kvantové sítě mohly v budoucnu také zapojit. Krok ČVUT je jedním ze signálů rostoucího zájmu o kvantové technologie v České republice. Česko rovněž buduje kvantovou síť pro přenos QKD klíčů a Národní superpočítačové centrum IT4Innovations v Ostravě se svým vlastním kvantovým počítačem. 



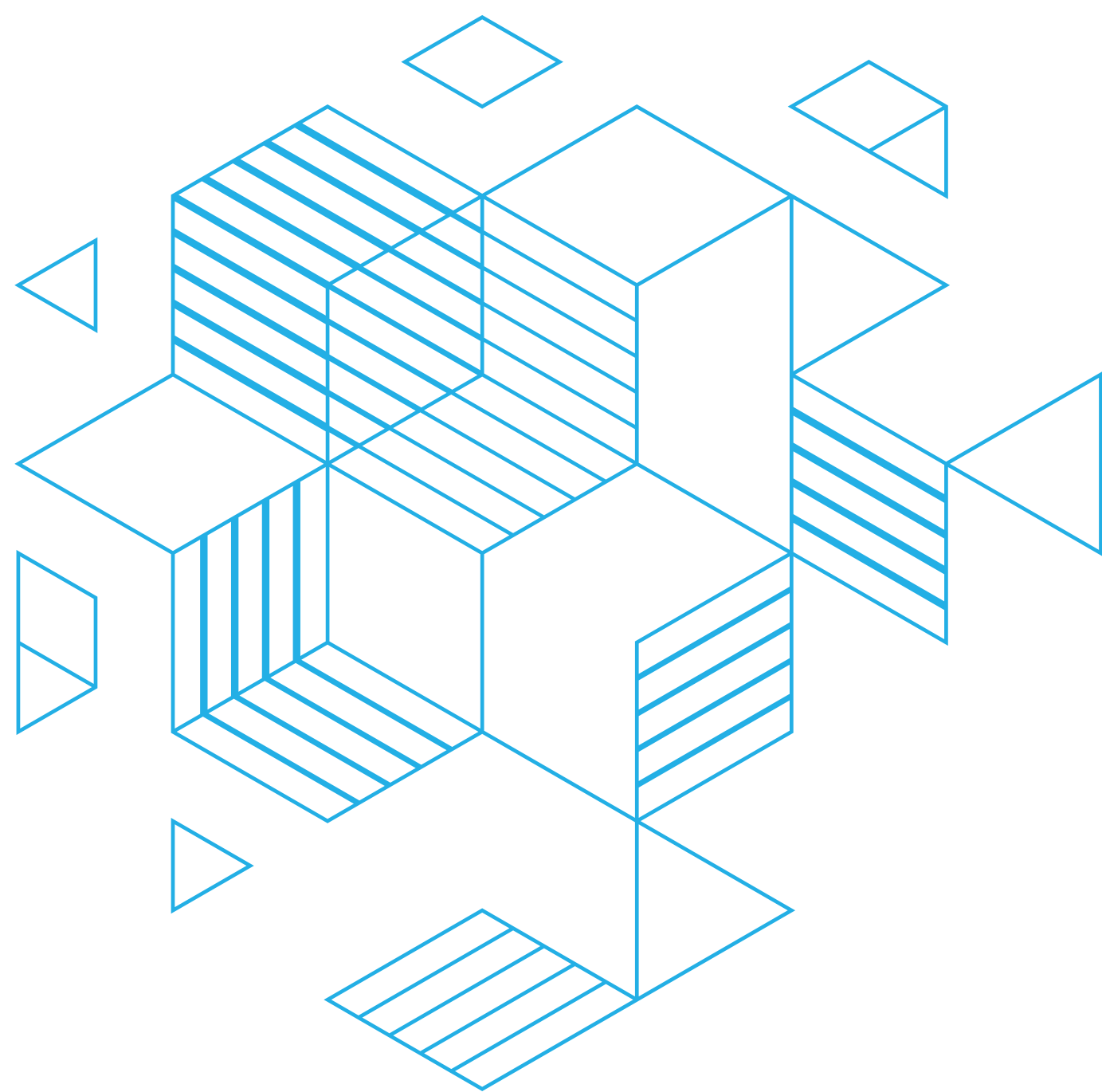
## Technologická agentura ČR vyhláší výzvy v programu SIGMA

V programu SIGMA **dílčí cíl 1, podpora komercializace VaVal+** byla vyhlášena již šestá veřejná soutěž, která je zaměřena právě na podporu komercializace průlomových inovačních řešení a růstu a rozvoje malých a středních podniků a start-upů se sídlem v Česku. Soutěž cílí na ověření praktického uplatnění výstupů aplikovaného výzkumu a jejich následnou přípravu na komerční využití. Lhůta pro podávání návrhů byla otevřena 17. ledna a bude ukončena 6. března 2024. Rovněž byla vyhlášena sedmá veřejná soutěž pro **dílčí cíl 2, začínající výzkumníci/výzkumnice**. Cílem je kromě zapojení začínajících výzkumnic a výzkumníků v oblasti aplikovaného výzkumu také podpora rovných příležitostí pro ženy a muže ve vědě. Soutěž je otevřená od 8. února do 27. března 2024. 



## Info den Evropského kompetenčního centra pro kybernetickou bezpečnost


Akce, jež představuje úvod k sérii zaměřené na poskytování informací o nadcházejících výzvách z programu Digitální Evropa, se uskutečnila 22. února 2024 v rumunské Bukurešti. Cílem je usnadnit přístup k informacím o evropských výzvách zaměřených na kyberbezpečnost a také zvýšení povědomí o současných i budoucích výzvách. Info den rovněž umožní široké veřejnosti setkat se se zástupci institucí, které možnosti financování zastřešují. ECCC tímto rovněž naplňuje závazek budovat silnější a propojenější evropskou komunitu v oblasti kybernetické bezpečnosti. [↗](#)




## Kybernetická aréna BUTCA získala Cenu ministra za mimořádné úspěchy v oblasti bezpečnostního výzkumu

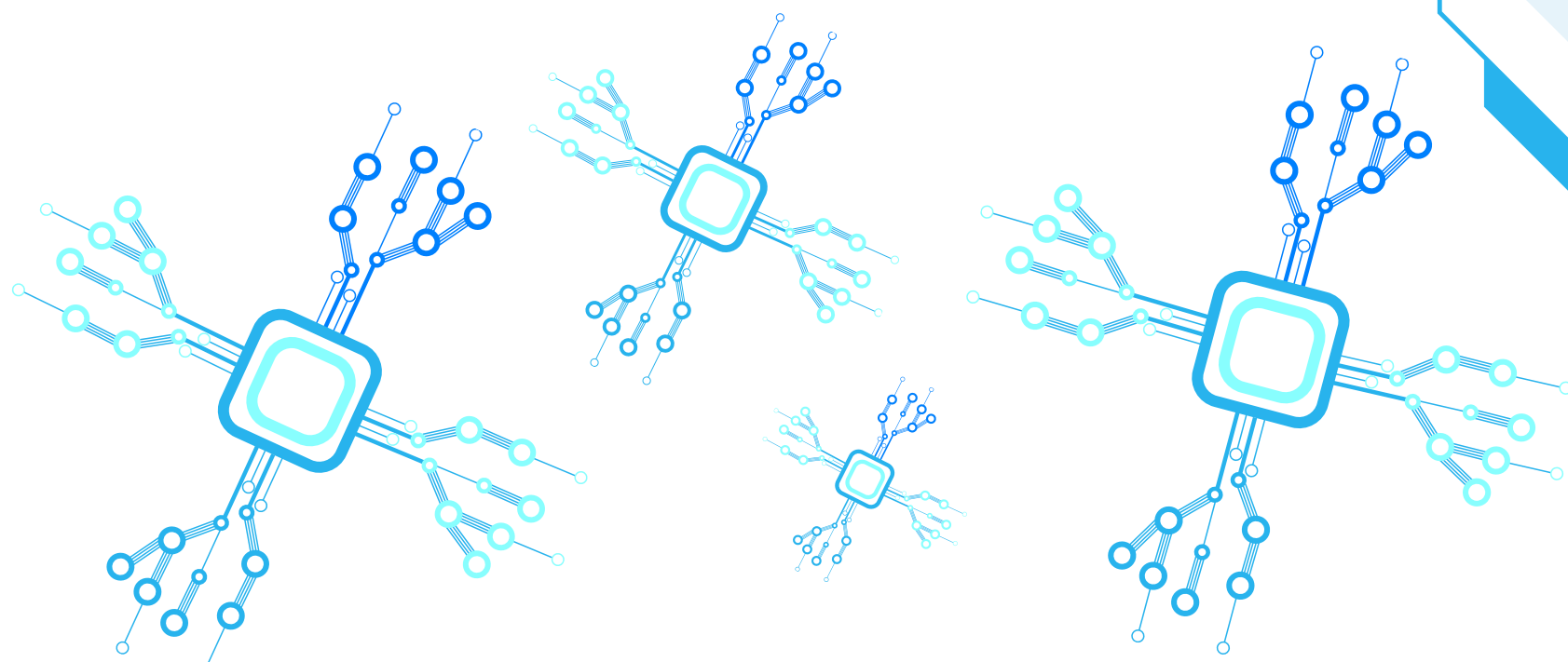
Cenu ministra vnitra za mimořádné výsledky v oblasti bezpečnostního výzkumu, vývoje a inovací pro rok 2023 získal projekt "Kybernetická aréna pro výzkum, testování a edukaci v oblasti kyberbezpečnosti", na kterém se podíleli zástupci Vysokého učení technického v Brně (VUT) v rámci Programu bezpečnostního výzkumu České republiky v letech 2015–2022. Kybernetická aréna BUTCA je platformou pro vzdělávání a školení, a to i pro studenty středních škol. Během prvního roku její existence byla využita k výuce více než tisícovky studentů. [↗](#)

## Fyzikům z Lipské univerzity se podařilo vytvořit neuronovou síť nevyžadující elektrické napájení

Umělá inteligence na bázi neuronové sítě obvykle provádí své výpočty digitálně pomocí mikroelektronických čipů. Fyzikům z Lipské univerzity se však podařilo vytvořit typ neuronové sítě, která nepracuje s elektrinou, ale s tzv. aktivními koloidními částicemi. Jedná se o částice, které jsou jemně rozptýlené ve svém disperzním prostředí (pevná látka, plyn nebo kapalina). Pro své experimenty vědci vyvinuli malé plastové jednotky obsahující zlaté nanočástice, v nichž jedna částice rotuje kolem druhé, poháněna laserem. Tyto jednotky mají jedinečné fyzikální vlastnosti a každá z nich má schopnost zpracovávat informace. Více jednotek dohromady tvoří tzv. rezervoár (reservoir computing). Stejně jako u jiných modelů neuronových sítí musí být systém vytrénován k provádění automatizovaných výpočtů. Vyvinutá metoda dokáže efektivně potlačit rušivé vlivy při pohybu koloidních částic, např. v podobě šumu. Efektivní využití principu rezervoárových výpočtů pak skrývá potenciál zvýšit výpočetní kapacitu hardwaru. Vyvinutá metoda může představovat další pokrok v procesu vývoje umělé inteligence a předpovídání časových řad. 


### Věděli jste, ŽE...

...vědecký časopis Nature zařadil do svého žebříčku nejvlivnějších osobností, které ovlivnili formování vědy v roce 2023, také ChatGPT? Do pravidelně vydávaného ocenění pro nejvlivnější osobnosti ve vědě za uplynulý rok autoři tentokrát připojili také nelidskou entitu v podobě známého jazykového modelu. ChatGPT měl na vědu a její vnímání skutečně obrovský vliv, kdy kromě výhod jako je psaní grantových žádostí, pomoc s hledáním mezery v současném poznání, či analyzování velkých souborů dat, zhmotnil také svá značná rizika v podobě nedostatečné ochrany dat a etických otázek. 



## Vědci vytvořili první funkční polovodič z grafenu využitelný v kvantových počítačích

Po letech výzkumu se vědcům z Georgia Institute of Technology podařilo vytvořit první funkční polovodič z grafenu. Struktura grafenu se skládá z nejpevnějších známých vazeb, díky čemuž je grafenový polovodič desetkrát pohyblivější než křemík a dokáže přenášet velmi vysoké proudy, aniž by se zahříval nebo rozpadal. Elektrony se pohybují s velmi malým odporem, což umožňuje zrychlení jejich výpočetní kapacity. Týmu vědců se podařilo překonat hlavní překážku využití grafenu v elektronice, tzv. pásmovou mezeru, která je klíčovou vlastností polovodičů a umožňuje jejich zapínání a vypínání. Grafen tuto vlastnost ve svém


přirozeném stavu postrádá a k jejímu získání je zapotřebí speciální proces, při kterém vzniká tzv. epitaxní grafen. Právě tento objev otevírá dveře k novému způsobu výroby elektroniky, protože křemík již naráží na své limity kvůli stále rostoucím nárokům na rychlost počítačů a velikost jejich součástek. Epitaxní grafen by proto podle vědců mohl znamenat změnu paradigmatu v elektronice a umožnit zcela nové technologie využívající jeho jedinečné vlastnosti. Materiál například umožňuje využít vlnové vlastnosti elektronů v kvantové mechanice, což je předpokladem pro fungování kvantových počítačů. 

„Nyní máme k dispozici extrémně odolný grafenový polovodič s desetinásobnou pohyblivostí oproti křemíku, který má navíc jedinečné vlastnosti, jež křemík nemá.“

**Walter de Heer**  
profesor fyziky na  
Georgijském technickém institutu


## Olomoučtí vědci pomohli vytvořit logický qubit se zabudovanou korekcí chyb

Mezinárodní skupina vědců z univerzit v Mainzi, Olomouci a Tokiu vytvořila první verzi Gottesman-Kitaev-Preskill kvantových kódů (GKP) pro volně se šířící světlo, čímž otevřela cestu ke konstrukci optických kvantových počítačů. Důležitou vlastností kvantových bitů, obdobou bitů klasických počítačů, je jejich odolnost vůči náhodným chybám. U kvantových počítačů je třeba odhalit a opravit i malé nepřesnosti, protože každá chyba by mohla mít dalekosáhlé důsledky. Standardním řešením tohoto problému je zakódování logických qubitů do větších fyzických qubitů, což však snižuje možnost začlenit je do větších obvodů. Tým výzkumníků se proto zaměřil na zakódování logických qubitů do optických oscilátorů, které jsou schopny zachovat odolnost proti chybám i při přenosu velmi složitých kvantových kódů. Tyto kódy lze vytvořit pomocí mikrovlnných kvantových obvodů, jednotlivých chladných atomů a díky zmíně-

nému úspěchu vědců i při pokojové teplotě, jako zvláštní stavy světla. Kód GKP se skládá z velkého počtu fotonů v jediném optickém impulsu, který má přesnou strukturu a fotony jsou uspořádány ve virtuální mřížce. Náhodné chyby mohou vést k deformaci nebo posunu virtuální mřížky, což lze detekovat a korigovat. Výsledky jejich práce již byly publikovány, a to v prestižním časopise Science. 

## Výzkumníci představili nový způsob boje proti útokům na převzetí účtu mobilního telefonu

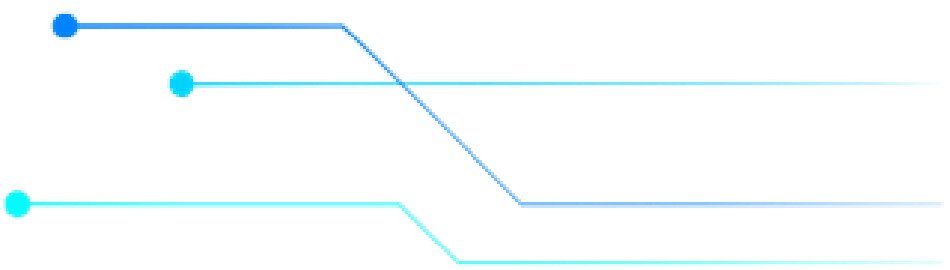
Mobilní telefony jsou složitým ekosystémem operačního systému a aplikací, což útočníkům otevírá dveře k využití dosud neobjevených bezpečnostních zranitelností k získání kontroly nad aplikacemi, nebo celým mobilním zařízením. Cílem útočníků je získat přístup k osobním údajům nebo bankovním účtům. Předcházet těmto útokům pomůže nová metoda identifikace bezpečnostních zranitelností, kterou vyvinuli počítačové vědci z univerzit v Birminghamu, Edinburghu, Surrey a Twente. Doposud se

bezpečnostní zranitelnosti zkoumaly pomocí tzv. grafů přístupu k účtům, které zobrazují telefon, SIM kartu, aplikace a bezpečnostní prvky, které omezují jednotlivé úrovně přístupu. Tato metoda však nepočítá s tím, že útočník může zařízení nebo aplikaci odpojit od účtu v ekosystému (Apple nebo Google). Může například vyjmout kartu SIM a vložit ji do jiného telefonu, aby získal přístup k SMS zprávám a pomocí metody obnovení hesla skrze SMS získal kontrolu nad účtem. Nová metoda zachycuje všechny potenciální schopnosti hackera, který má přístup k mobilnímu telefonu a kódu PIN, a umožňuje tak zachytit snahu o odcizení dat i po vyjmutí karty SIM nebo odpojení účtu od elektronického ekosystému. Nyní je využití tohoto postupu detekce na výrobcích zařízení. 

### Tipy na zajímavé akce

Únor

- 23. - Seminář s předsedou GA ČR v Praze
- 27. - 21. ročník konference České dny pro evropský výzkum (CZEDER)
- 27. - 6G Horizon session at Mobile World Congress 2024
- 27. - CONNECT University Online Session



Národní úřad  
pro kybernetickou  
a informační bezpečnost

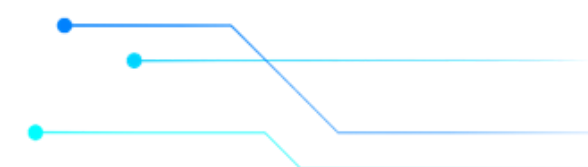
Mučednická 1125/31

616 00 Brno

Tel.: +420 541 110 777

P.O. BOX 17, Brno 16, CZ 616 00

Oddělení vědy, výzkumu  
a inovací



Olšanská 36/9

130 00 Praha

Tel.: +420 607 032 806

e-mail: [vyzkum@nukib.cz](mailto:vyzkum@nukib.cz)

