Pokud Čína prolomila americké šifrování, proč by nám to řekla?

nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/if-china-cracked-us-encryption-why

28. ledna 2023

Když Alan Turing prolomil kód Enigmy během druhé světové války, ani Spojené království, ani Spojené státy okamžitě nezveřejnily dokument oznamující úspěch. Místo toho si to nechali pro sebe, aby mohli dál číst nacistické zprávy zašifrované pomocí strojů Engima. Naproti tomu minulý měsíc čínští akademici z vládních laboratoří a výzkumných organizací zveřejnili článek , v němž tvrdí, že vyvinuli novou matematickou strategii k prolomení šifrování RSA, dnešního standardu.

Pokud čínská vláda dokáže prolomit šifrování RSA, pak se může nabourat do každého systému americké vlády a soukromého sektoru, vidět a exfiltrovat cokoli a všechno a dosáhnout skutečné informační dominance nad Washingtonem a jeho spojenci a partnery.

Existují však důvody k pochybnostem o přesnosti tvrzení listu a ještě více důvodů k pochybnostem, proč by čínští vědci ukazovali ruku, kdyby skutečně prolomili naše kódy.

Jednoho dne počítačoví vědci *prolomí* šifrování RSA. Než se tak ale stane, budou muset mít ty správné nástroje. Na základě současného chápání matematiky bude prolomení šifrování RSA vyžadovat

kvantové počítače, které využívají principy kvantové fyziky k exponenciálnímu urychlení řešení problémů.

Závod o kvantové výpočty je v plném proudu. V listopadu IBM uvedla na trh dosud největší kvantový počítač, Osprey. Tento milník „nás o krok blíže“ k „nadcházející éře kvantově centrických superpočítačů,“ řekl ředitel výzkumu IBM . Osprey však zatím nedokáže vyřešit složité matematické problémy, kterým čelí ti, kteří chtějí prolomit šifrování RSA. Peking však tvrdí, že dokáže prolomit šifrování RSA hybridním přístupem, který kombinuje klasické výpočty a kvantové výpočty pomocí menšího kvantového počítače.

Pokud by Čína skutečně prolomila šifrování RSA, neřekli by nám to. Možná se Čína snaží získat místo u stolu a hledá pozvání ke spolupráci s kvantovými výzkumnými zařízeními v zámoří. Tyto pozvánky mohly vyschnout poté, co Washington uzákonil řadu politik blokujících sdílení kvantových technologií s Čínou kvůli kvantovým vojenským aplikacím. Pokud by však cílem byly pozvánky, autoři čínského listu se možná střelili do nohy, když odhalili, že za zahraničními konkurenty roky zaostávají. Přístup, který vědci uplatňují ve svém článku, je podobný přístupu popsanému v jiném článku publikovaném před pěti lety americkou společností zabývající se kvantovým softwarem, vysvětlujeKevin Kane, generální ředitel American Binary, společnosti zabývající se kybernetickou bezpečností zaměřenou na bezpečnost v kvantové éře.

Peking již dříve zveřejnil to, co se zdá být špičkovým výzkumem ve snaze získat chválu, aby byl později tento výzkum odhalen. Zdá se, že to platí znovu. Řada kvantových a počítačových expertů již vyjádřila pochybnosti o zjištěních nového článku. Matematická strategie, kterou dokument zkoumá, není škálovatelná na velmi velká čísla, vysvětluje Kane. Nicméně varuje, že pokud je dokument pravdivý, znamená to, že Čína je dále, než jsme si mysleli, a dělá významný pokrok. Profesor informatiky z University of Austin Scott Aaronson

mezitím panuječínští akademici za zavádějící tvrzení, že jejich přístup je rychlejší než klasická výpočetní technika, i když to ve skutečnosti vypadá, že tomu tak není.

Vzhledem k rozsahu hrozby by však bylo nebezpečné odmítat čínská tvrzení jako pouhé vychloubání. Odložte na chvíli otázku, zda matematika funguje, nebo ne. Proč by Čína obětovala významnou strategickou výhodu za práva akademického vychloubání?

Možná se čínská vláda snaží přesvědčit svět, že prolomila šifrování RSA, aby vytvořila určitý druh odstrašení. Pokud někdo opakuje nepravdivé informace dostatečně často, ostatní tomu mohou začít věřit, zvláště pokud se ze začátku bojí. Kvantový papír by mohl být součástí série snah přesvědčit Spojené státy, že Čína získala nepřekonatelnou technologickou převahu. Peking možná sází na to, že američtí tvůrci rozhodnutí, tváří v tvář silnějšímu protivníkovi, podřídí vůli Číny v různých globálních otázkách.

Rozpoznat motivaci Pekingu může být náročné, ale měli bychom si připomenout slova Sun Tzu: „Ti, kdo jsou zkušení ve válčení, hýbou nepřítelem a nepřítel je nepohne.“ Pekingští strategickí plánovači nepochybně sledují, jak Amerika a její spojenci zareagují – do jaké míry se Washington angažuje, do jaké míry reaktivního chování a do jaké míry rezignace. Čínští akademici možná odhalili svou ruku, ale Washington by neměl. Součástí amerického hodnocení jejích příštích kroků by mělo být hodnocení toho, jaké ponaučení by se Čína mohla naučit z toho, jak americká vláda zareaguje.

Bez ohledu na to, proč byl článek publikován, se rychle blíží den, kdy kvantové počítače prolomí dnešní šifrování. Amerika a její spojenci musí nejprve dosáhnout tohoto milníku a zároveň zvýšit bezpečnostní a šifrovací standardy, aby se chránili před protivníkem s pokročilými schopnostmi prolomit šifrování. Oba tyto kroky vyžadují vládní a soukromé investice do kvantového výzkumu a vývoje a do kultivace kvalifikované pracovní síly potřebné k provádění tohoto výzkumu a realizaci řešení.

Dr. Georgianna Shea je hlavní technologkou Centra pro kybernetické a technologické inovace (CCTI) při Nadaci pro obranu demokracií (FDD).

Annie Fixler je ředitelkou CCTI a výzkumným pracovníkem FDD. Sledujte Annie na Twitteru @afixler .

Obrázek: Flickr/IBM Research.