Kas tehisaru murdis just interneti krüpteeringu?

30 min tagasi - 28.11.2026 Autor: AM

Teadusmaailmas liiguvad ärevad kuuldused, et Silicon Valley juhtivad tehisarulaborid võivad olla leidnud viisi, kuidas lahti murda avaliku ja salajase võtmega krüpteeringut. Seni peeti seda hüputeetiliselt võimalikuks juhul, kui õnnestub tööle saada piisavalt töökindel kvantarvuti..

Texase ülikooli arvutiteadlane Scott Aaronson, keda tuntakse pigem kaine ja skeptilise meelega teadlasena, avaldas oma blogis postituse, mille pealkiri räägib enda eest: „HOLY SHIT HOLY SHIT HOLY SHIT HOLY SHIT“ (eesti keeles viisakamalt: „Püha püss!“). Tema sõnul istuvad OpenAI ja Anthropic mitme usaldusväärse allika kinnitusel ühe või mitme tõelise „pommuudise“ otsas.

Kuigi täpsed detailid on veel udused, kardetakse, et tehisaru loodud algoritmid võivad üsna pea murda avaliku võtme krüptograafia.

Õhtusöögilauas oodati uut teadusrevolutsiooni enne magustoitu

See, mis praegu matemaatikas ja arvutiteaduses toimub, meenutab Aaronsoni sõnul hetke, mil Galileo esimest korda teleskoobi tähtede poole suunas. Ta kirjeldab värvikalt, kuidas istus koos sõprade ja kolleegidega õhtusöögilauas, telefonid ja sülerid laual laiali, oodates hinge kinni pidades, milline uudis järgmisena kukub. OpenAI ja Anthropic ei vaevu enam isegi pressiteateid saatma – nad lihtsalt laadivad oma GitHubi lehtedele üles teadustöid, mis lahendavad aastakümneid püsinud mõistatusi.

Enne kui magustoit lauale jõudis, selgus, et OpenAI tehisaru oli tõestanud maatriksite korrutamise eksponendi täpse väärtuse (9/4) ning parandanud 1960. aastatest püsinud kiire Fourier' teisenduse piire. Ja seda kõike vahetult pärast seda, kui avalikkust olid šokeerinud tehisaru abil sündinud Riemanni hüpoteesi ja keerukusteooria (VP ≠ VNP) tõestused.

Kõik need „iidsed“ küsimused, millele inimesed vastuseid otsisid, saavad nüüd korraga lahenduse.

Kui varem võis skeptik käega lüüa ja arvata, et tegu on järjekordse juturoboti hallutsinatsiooniga, siis enam see nii lihtne pole. Laborid varustavad oma tööd

Lean-tõestussertifikaatidega. See on automaatne matemaatiline kontrollsüsteem, mis ei lase vigasel loogikal läbi lipsata – umbes nagu ülitäpne audiitor, kes ei usu ilusat juttu, vaid kontrollib iga viimse kui tehte üle.

Kas pangaäpp ja paroolid ongi nüüd ohus?

Kõige enam kütab kirgi küsimus, kas tehisaru on tõesti leidnud viisi, kuidas murda väga laialt levinud RSA-krüpteeringut.

RSA turvalisus põhineb lihtsal ideel: kahe hiiglasliku algarvu korrutamine on arvutile käkitegu, kuid tulemuse tagasi algarvudeks lahutamine võtab tavalise arvutiga aega sisuliselt igaviku. See on nagu värvide segamine – kokku segada on lihtne, aga algseid toone hiljem eraldada peaaegu võimatu.

Kuulduste järgi on tehisarulaborid leidnud algoritmid, mis suudavad selliseid ülesandeid lahendada polünomiaalses ajas. See tähendab, et pikema parooli või võtme murdmiseks kuluv aeg ei kasva enam plahvatuslikult, vaid palju rahulikumalt ja prognoositavamalt.

Kas kogu internet kukub nüüd homme kokku? Mitte ilmtingimata. Isegi kui algoritm on paberil „kiire“, võib see päriselus olla ikkagi liiga aeglane, et pikki krüptovõtmeid praktikas murda.

Kuid nagu Aaronson ajakirjale Nature nentis:

> „Probleem on selles, et usk, nagu oleks see ülesanne raske, on surnud.“

Ajalugu näitab, et kui uks on kord irvakile lükatud, leiab keegi peagi viisi, kuidas see pärani lahti lüüa.

Kas kogu krüptograafia on hukule määratud?

Kõige mustem stsenaarium eeldaks, et tõeks osutub arvutiteaduse kuulus küsimus P = NP ehk iga ülesanne, mille vastust on lihtne kontrollida, on ka lihtsalt lahendatav. Sellisel juhul oleks peaaegu kogu tänapäevane krüptograafia tõepoolest ohus. Õnneks peab enamik teadlasi seda endiselt ebatõenäoliseks.

Veelgi enam: OpenAI ja Anthropicu värsked tulemused annavad isegi põhjust ettevaatlikuks optimismiks. Need viitavad, et paljud keerulised arvutusprobleemid ongi fundamentaalselt rasked. MIT-i arvutiteadlane Ryan Williams tunnistas Nature´ile, et on viimastest arengutest pahviks löödud – tehisaru on loonud täiesti

uue raamistiku, mille abil tõestada arvutamise piire. See tähendab, et matemaatika ise võib meile appi tulla ja pakkuda vanade lukkude asemele uusi ja veelgi kindlamaid.

Singulaarsuse algus või lihtsalt uus ajastu?

Kuigi sotsiaalmeedias leidub endiselt kriitikuid, kes üritavad tehisaru tõestusi pisidetailide põhjal kahtluse alla seada, on Aaronson veendunud, et silmi ei saa enam kinni pigistada. Tema sõnul tundub viimane nädal täpselt selline, nagu ta on alati ette kujutanud tehisaru singulaarsuse algust. Jääb vaid loota, et see piirdub esialgu „kõigest“ väga raskete matemaatikaülesannete lahendamisega.

- Uudised

- Tehisintellekt
- Tarkvara

Pilt

