

Sistemi di Crittografia sotto pressione - Transazioni bancarie e Sicurezza digitale in pericolo

Pubblicato il 28/11/2026

Un'inchiesta del *Guardian* datata 28 novembre 2026 ha acceso i riflettori su possibili svolte matematiche maturate all'interno dei laboratori di intelligenza artificiale, potenzialmente in grado di mettere **sotto pressione i sistemi di crittografia alla base della sicurezza digitale globale**. Le indiscrezioni — riportate anche dal lancio LaPresse da Francoforte — riguardano risultati non ancora resi pubblici che, se verificati e tradotti in applicazioni pratiche, potrebbero esporre transazioni bancarie, comunicazioni diplomatiche, messaggi riservati e connessioni protette.

Cosa emerge dalle fonti e dalle verifiche

Le voci circolate tra ricercatori e addetti ai lavori si concentrano su due livelli distinti: da un lato l'ipotesi di scoperte matematiche riservate sui fondamenti della crittografia, dall'altro il clima di

forte accelerazione vissuto dalla matematica assistita dall'intelligenza artificiale nelle ultime settimane.

- **Le indiscrezioni sui laboratori:** L'informatico teorico Scott Aaronson (Università del Texas ad Austin, con trascorsi di ricerca in OpenAI) ha dichiarato al *Guardian* e sul proprio blog di ritenere plausibile, sulla base di più fonti affidabili, che grandi laboratori come OpenAI e Anthropic dispongano di risultati crittografici non ancora annunciati. Allo stesso tempo, ha chiarito di non aver visto prove verificate per le voci più allarmistiche — come un algoritmo rapido e generale per la fattorizzazione in tempo polinomiale capace di scardinare subito standard come RSA.
- **Due esiti possibili:** Secondo gli esperti citati dal quotidiano britannico, un'eventuale scoperta matematica non significa necessariamente un nuovo metodo per violare i cifrari. Potrebbe anche dimostrare l'inesistenza di determinate scorciatoie computazionali, rafforzando di fatto la fiducia nella solidità teorica di alcuni sistemi esistenti.
- **Il contesto matematico:** L'allarme si inserisce in una fase di forte fermento per la ricerca matematica legata ai modelli di IA, tra dimostrazioni recenti su questioni di complessità computazionale e progressi su problemi storici come l'ipotesi di Riemann. Sul piano delle difese, intanto, prosegue il lavoro sulla crittografia post-quantistica, tradizionalmente pensata per fronteggiare futuri computer quantistici più che scoperte algoritmiche improvvise.

Nessuna compromissione confermata, ma serve agilità

Al momento **nessuna azienda ha confermato** di aver violato protocolli crittografici in uso e qualsiasi eventuale dimostrazione dovrà superare il vaglio indipendente della comunità scientifica. Gli specialisti sottolineano che il passaggio da un risultato teorico a un attacco funzionante su infrastrutture reali non è automatico né immediato.
Il punto critico indicato dagli esperti riguarda piuttosto i tempi di aggiornamento: **banche, amministrazioni pubbliche e operatori critici che faticano a migrare verso nuovi standard** rischiano di trovarsi esposti se i tempi si accorciassero rispetto alle tabelle di marcia previste per la transizione crittografica.

Link notizia: https://www.theguardian.com/europe