**Rewolucja w szyfrowaniu – kwantowy generator liczbowy w akcji!**

**Firma Pancernik it informuje iż naukowcy z Quantum Base, przy współpracy z Uniwersytetem Lancaster, stworzyli pierwszy praktyczny kwantowy generator liczb, który może w szybki i płynny sposób współpracować niemalże z każdym urządzeniem zawierającym nowoczesne oprogramowanie (np. poprzez wpięcie dodatkowego chipa w półprzewodniki).**

Firma Pancernik it informuje iż naukowcy z Quantum Base, przy współpracy z Uniwersytetem Lancaster, [stworzyli pierwszy praktyczny kwantowy generator liczb](https://interestingengineering.com/first-practical-quantum-random-number-generator-could-revolutionize-internet-security), który może w szybki i płynny sposób współpracować niemalże z każdym urządzeniem zawierającym nowoczesne oprogramowanie (np. poprzez wpięcie dodatkowego chipa w półprzewodniki). Szef firmy Quantum Base, Phillip Speed (cóż za nazwisko! – dop. autor) powiedział:

„Stworzyliśmy małe, ergonomiczne narzędzie, które wytwarza w pełni losowe liczby. Może być wdrożone w każdy elektroniczny produkt, niedużym lub nieprzyrostowym kosztem, przy osiągnięciu odpowiedniej wielkości produkcji”.

Obecna „losowość” liczb w technologiach szyfrowania jest tylko pozorna. Każdy system kieruje się odpowiednim algorytmem, który może posiadać swoje luki. Tak było chociażby w 2017 roku w Estonii, gdy [cyfrowe dowody osobiste mogły zostać skopiowane/skradzione](https://www.schneier.com/blog/archives/2017/09/security_flaw_i.html) w wyniku luki systemowej w takich algorytmach.

Z drugiej strony, kwanty które nie poddają się sztywnym i zdeterminowanym zasadom fizyki ogólnej, a których zachowanie jest kompletnie nieprzewidywalne, wydają się świetnym źródłem losowości. I tak jest w przypadku kwantowych generatorów liczb, które wykorzystują specyfikę tych małych cząsteczek. Zapewne niebawem rozwiązanie Quantum Base i Uniwersytetu Lancaster znajdzie zastosowanie w niemalże każdym sprzęcie i oprogramowaniu. Technologie typu blockchain, kryptowaluty, czy transmisje szyfrowane, będą w praktyce nie do przejęcia.

Źródła:

[blog.pancernik.it](http://pancernik.biuroprasowe.pl/word/?hash=8a65817a7df5f54895e472c4a92d4fc8&id=86613&typ=eprblog.pancernik.it)

[interestingengineering.com](http://pancernik.biuroprasowe.pl/word/?hash=8a65817a7df5f54895e472c4a92d4fc8&id=86613&typ=eprinterestingengineering.com)

[csoonline.com](http://pancernik.biuroprasowe.pl/word/?hash=8a65817a7df5f54895e472c4a92d4fc8&id=86613&typ=eprcsoonline.com)

[schneier.com](http://pancernik.biuroprasowe.pl/word/?hash=8a65817a7df5f54895e472c4a92d4fc8&id=86613&typ=eprschneier.com)