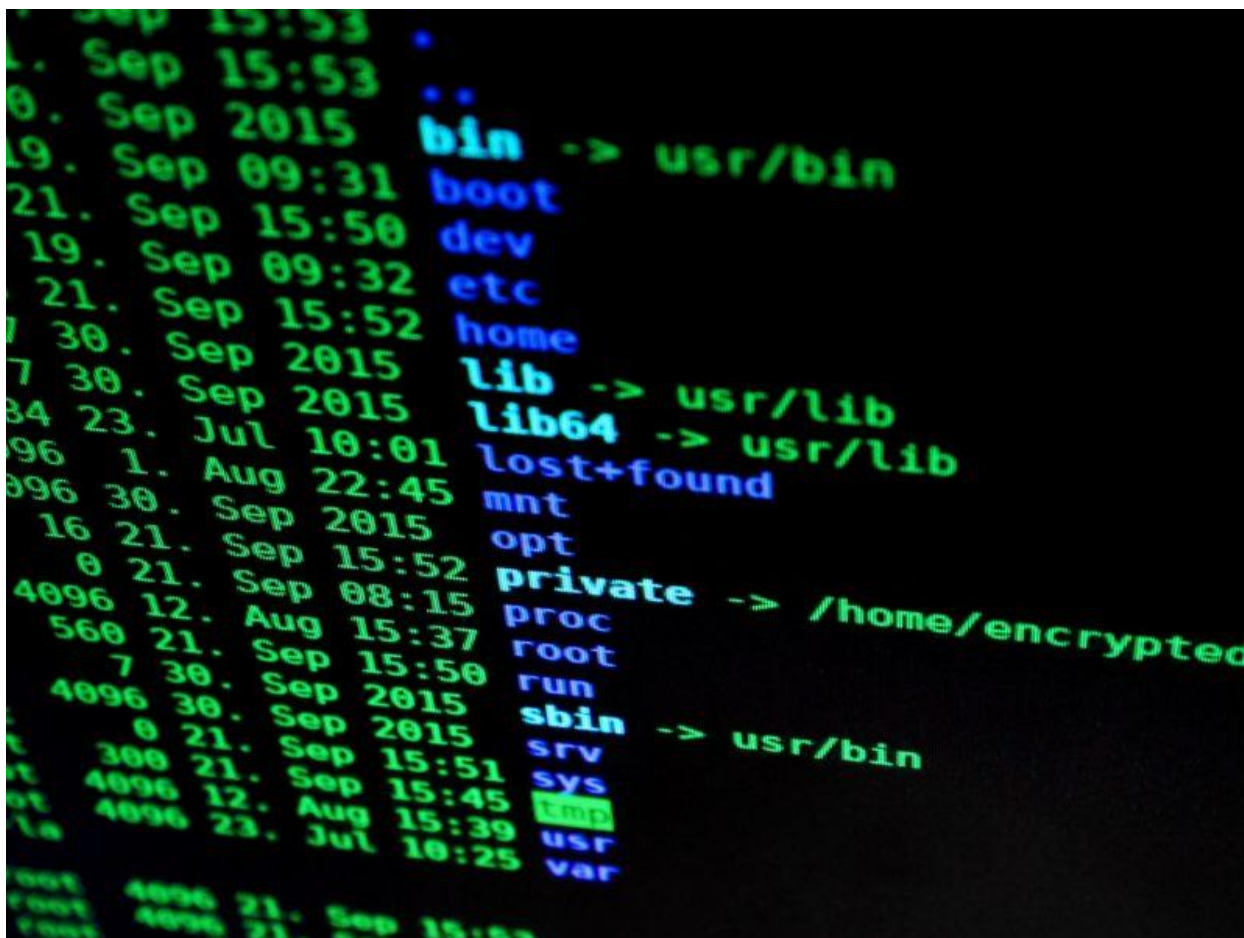


Katowice 11.12.2018



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). 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](#) w wyniku luki systemowej w takich algorytmach.

Tel.(32) 32 745 46 03
KRS:KRS 0000520895
REGON:243673423
NIP:634-283-09-89

Pancernik it sp. z o.o.
ul. Paderewskiego 35
40-282 Katowice
biuro@pancernik.it
www.pancernik.it

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 przejścia.

Źródła:

blog.pancernik.it

interestingengineering.com

csoonline.com

schneier.com