

CHIŃSKI SATELITA DO KOMUNIKACJI KWANTOWEJ ROZPOCZĄŁ DZIAŁALNOŚĆ OPERACYJNĄ

Satelita QUESS jest w zasadzie demonstratorem technologii. Urządzenie będzie służyć próbom kwantowej transmisji danych. Metody komunikacji testowane przez chiński pojazd kosmiczny oferują niezwykle wysoki poziom ochrony przesyłanych informacji przed atakiem hakerskim.

Satelita telekomunikacyjny QUESS (Quantum Experiments at Space Scale), zwany też Micius, [został wystrzelony na orbitę 15 sierpnia 2016 r. z użyciem rakiety Chang Zheng-2D \(pol. Długi Marsz-2D\)](#). Udany start przeprowadzono z Centrum Startowego Satelitów Jiuquan w prowincji Gansu, ulokowanego na pustyni Gobi w północnej części Chin. Przez ostatnie cztery miesiące trwały próby podzespołów satelity, kanałów komunikacji z urządzeniem oraz obsługującej go infrastruktury naziemnej.

Wreszcie, Chińska Akademia Nauk (CAS), w której laboratoriach QUESS powstawał, podała, że testy zostały zakończone i można przystąpić do realizacji właściwej części misji. Chińczycy poinformowali, że urządzenie działa prawidłowo, zgodnie z oczekiwaniami. Jak poinformował Pan Jianwei, naukowy szef projektu, udało się już przeprowadzić z udziałem satelity pierwsze transmisje danych z prawdziwego zdarzenia i uzyskać pierwsze informacje na temat działania systemu.

„Satelita Quantum Experiments at Space Scale (QUESS) to pierwsza w historii kosmiczno-naziemna platforma testowa do komunikacji kwantowej” - podkreślił Wang Jianyu, zastępca głównego inżyniera projektu.

Komunikacja kwantowa polega na kodowaniu informacji w oparciu o przypisanie ich do określonych konfiguracji cząstek subatomowych i ich parametrów fizycznych, tzw. stanów kwantowych. Podstawową jednostką zapisu danych jest w tym przypadku bit kwantowy, czyli kubit (ang. quantum bit, qubit), odpowiednik bitu w komunikacji cyfrowej. W wymiarze praktycznym zastosowanie znajduje transmisja z wykorzystaniem fotonów w odpowiednio zakodowanych stanach kwantowych. Wśród podstawowych protokołów kwantowej dystrybucji klucza wyróżnia się metodę opartą na zjawisku splątania kwantowego, w którym występuje współzależność stanów własnych cząstek subatomowych pozostających ze sobą w powiązaniu.

Komunikacja kwantowa zapewnia niespotykaną dotąd jakość szyfrowania przekazywanych informacji, gwarantując niewrażliwość na obecnie stosowane formy ataków hakerskich i włamań. System zawdzięcza swoją odporność samej specyfice zjawisk kwantowych, które umożliwiają wykorzystanie cząstek subatomowych w roli nośnika zaszyfrowanej informacji. Próba jej odczytania przez podmiot nieupoważniony powoduje każdorazowo zmianę stanu kwantowego, który prowadzi do utraty pierwotnych danych, stając się zarazem sygnałem niepowołanej ingerencji.