CENTRE FOR JOINT WARFARE STUDIES

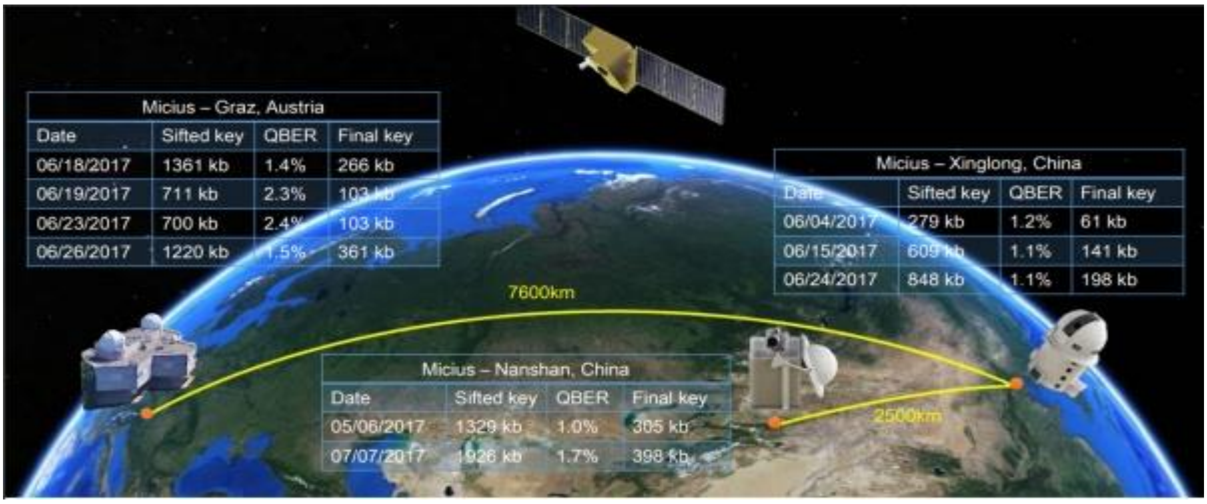
Aligned with the Future ★ Victory through Joint Knowledge ★

CENJOWS

QUANTUM SPACE TECHNOLOGY – 'MICIUS' SATELLITE

MICIUS: Chinese Quantum Satellite for Secured Communication. Quantum communication is guaranteed to be secure communication but it has never been possible over long distances as even the best optical fibers can carry photons only around 200 kilometers before light absorption makes the process impossible. A satellite, nicknamed Micius or Mozi (Chinese: 墨子) after the ancient Chinese philosopher and scientist, launched in 2016 and is operated by the Chinese Academy of Sciences, has made it possible. It working along with the University of Vienna and the Austrian Academy of Sciences has carried out secured communication with quantum encryption which is far more secure than the conventional encryption.

It is long known that quantum computers will be able to break almost all other types of cryptography. Since these devices are becoming more capable, the writing is on the wall for conventional encryption. So commercial businesses, governments, and the military are all waiting with bated breath for practical quantum cryptography systems to be developed.



Micius – Graz, Austria

Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China

Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

Micius – Nanshan, China

Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb

Chinese satellite the Micius has set up the first intercontinental quantum cryptography service. Researchers have tested the system by setting up a secure videoconference between Europe and China.

The process is straightforward. Quantum cryptography relies on what's called a one-time pad to guarantee privacy. This is a set of random numbers—a key—that can be used by two parties to encode and decode a message. The problem with one-time pad is in ensuring that only the selected transmitter and the receiver have them. This problem is solved by sending the key using quantum particles such as photons, since it is always possible to tell whether a quantum particle has been previously observed. If it has, the key is abandoned and another sent until both parties are sure they are in possession of an unobserved one-time pad.

The quantum key distribution is a crucial at the heart of quantum cryptography. After both parties have the key i.e. the one-time pad, they can communicate over ordinary classic channels with perfect security.

The Micius satellite simply distributes this key from orbit. Because it is in a sun-synchronous orbit over the poles, the satellite passes over every part of the Earth's surface at roughly the same local time each day. Say when the satellite is over the Chinese ground station at Xinglong in China's Northern Hebei province, it sends the one-time pad to the ground, encoded in single photons using a well-established protocol. As the Earth rotates beneath the satellite and as the ground station at Graz in Austria comes into view, Micius sends the same one-time pad to the receiver there. The two locations then both possess the same key that allows them to initiate completely secure communication over a classic link.

The experiment goes even one step further. If the goal is set up for a videoconference between the Chinese Academy of Sciences in Beijing and the Austrian Academy of Sciences in Vienna, so the key has to be distributed securely to both these locations. For this, the teams use ground-based quantum communication over optical fibers.

Video link so established is secured by the Advanced Encryption Standard (AES) that is refreshed every second by 128-bit seed codes. In September, they held a pioneering videoconference that lasted for 75 minutes with a total data transmission of roughly two gigabytes.

"We have demonstrated intercontinental quantum communication among multiple locations on Earth with a maximal separation of 7,600 kilometers," say the teams, which are led by Anton Zeilinger at the University of Vienna and by Jian-Wei Pan at the University of Science and Technology of China in Hefei, China.

There are some potential weaknesses in the system to work on for the future. Perhaps the most significant is that the satellite is considered secure during the time it takes to connect the two ground stations. That may well be true—who could hack an orbiting satellite? But, this security is not guaranteed. However, the teams say that this can be addressed in future designs with an end-to-end quantum relay.

National governments, military operators, and commercial businesses are all are keen for a similar secure capability. [1]

[1] ***https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/***