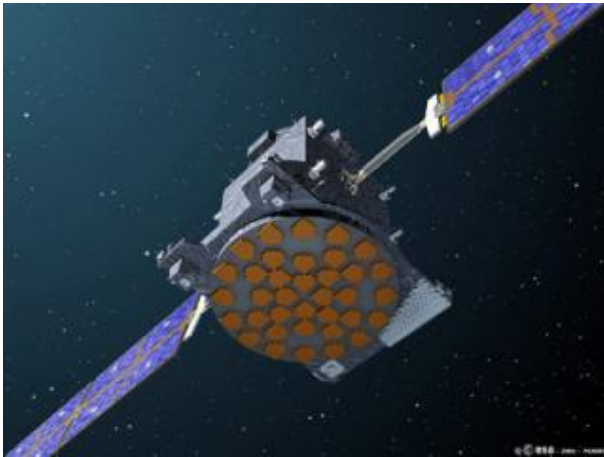


Cracking the secret codes of Europe's Galileo satellite



Artist's impression of GIOVE-A in orbit. Credits: ESA

Members of Cornell's Global Positioning System (GPS) Laboratory have cracked the so-called pseudo random number (PRN) codes of Europe's first global navigation satellite, despite efforts to keep the codes secret. That means free access for consumers who use navigation devices -- including handheld receivers and systems installed in vehicles -- that need PRNs to listen to satellites.

The codes and the methods used to extract them were published in the June issue of *GPS World*.

The navigational satellite, GIOVE-A (Galileo In-Orbit Validation Element-A), is a prototype for 30 satellites that by 2010 will compose Galileo, a \$4 billion joint venture of the European Union, European Space Agency and private investors. Galileo is Europe's answer to the United States' GPS.

Because GPS satellites, which were put into orbit by the Department of Defense, are funded by U.S. taxpayers, the signal is free -- consumers need only purchase a receiver. Galileo, on the other hand, must make money to reimburse its investors -- presumably by charging a fee for PRN codes. Because Galileo and GPS will share frequency bandwidths, Europe and the United States signed an agreement whereby some of Galileo's PRN codes must be "open source." Nevertheless, after broadcasting its first signals on Jan. 12, 2006, none of GIOVE-A's codes had been made public.

In late January, Mark Psiaki, associate professor of mechanical and aerospace engineering at Cornell and co-leader of Cornell's GPS Laboratory, requested the codes from Martin Unwin at Surrey Space Technologies Ltd., one of three privileged groups in the world with the PRN codes.

"In a very polite way, he said, 'Sorry, goodbye,'" recalled Psiaki. Next Psiaki contacted Oliver Montenbruck, a friend and colleague in Germany, and discovered that he also wanted the codes. "Even Europeans were being frustrated," said Psiaki. "Then it dawned on me: Maybe we can pull these things off the air, just with an antenna and lots of signal processing."

Within one week Psiaki's team developed a basic algorithm to extract the codes. Two weeks later they had their first signal from the satellite, but were thrown off track because the signal's repeat rate was twice that expected. By mid-March they derived their first estimates of the code, and -- with clever detective work and an important tip from Montenbruck -- published final versions on their Web site (<http://gps.ece.cornell.edu/galileo>) on April 1. The next day, NovAtel Inc., a Canadian-based major manufacturer of GPS receivers, downloaded the codes from the Web site and within 20 minutes began

tracking GIOVE-A for the first time.

Galileo eventually published PRN codes in mid-April, but they weren't the codes currently used by the GIOVE-A satellite. Furthermore, the same publication labeled the open source codes as intellectual property, claiming a license is required for any commercial receiver. "That caught my eye right away," said Psiaki. "Apparently they were trying to make money on the open source code."

Afraid that cracking the code might have been copyright infringement, Psiaki's group consulted with Cornell's university counsel. "We were told that cracking the encryption of creative content, like music or a movie, is illegal, but the encryption used by a navigation signal is fair game," said Psiaki. The upshot: The Europeans cannot copyright basic data about the physical world, even if the data are coming from a satellite that they built.

"Imagine someone builds a lighthouse," argued Psiaki. "And I've gone by and see how often the light flashes and measured where the coordinates are. Can the owner charge me a licensing fee for looking at the light? ... No. How is looking at the Galileo satellite any different?"

Source: Cornell University

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.