WAS QUANTUM ENTANGLEMENT EXPERIMENT BEHIND “CLASSIFIED CRYPTOGRAPHIC EQUIPMENT” CONFUSION AFTER ANTARES CRASH?

Yesterday evening, an Antares rocket built and operated by Orbital Sciences Corporation exploded shortly after liftoff. The rocket was intended to ferry supplies and equipment to the International Space Station. Orbital and Spacex have taken over some of the duties supplying the space station since the termination of NASA’s shuttle program.

In the early aftermath of the explosion, word came out that the crash site had to be secured because sensitive cryptographic equipment was on board:

> The Cygnus mission was non-military, but the company’s Antares program manager, Mike Pinkston, said the craft included “some classified cryptographic equipment, so we do need to maintain the area around the debris in a secure manner”.

That initially struck me as odd. The International Space Station has a large number of cooperating countries, including Russia. It’s hard to imagine that the US would put sensitive equipment into the hands of cosmonauts right now, given the cool state of US-Russian relations. Of course, it would make sense for ISS communications to be encrypted in order to prevent meddling by hackers, but movement all

the way to classified (and presumably military or NSA-level) encryption seems to be excessive.

This morning, we are seeing walk-back on the presence of classified equipment:

> Shortly after the explosion, CNN quoted a launch director as saying that the spacecraft contained classified “crypto” equipment, but early Wednesday a NASA spokesman said by email that “We didn’t have any classified items on board.”

In trying to make sense of what could have been behind these strange statements, I ran across this interesting announcement of a new cryptographic technology that European scientists have proposed evaluating in an experiment on the space staion:

> A team of European researchers have proposed a series of experiments that, if successful, could turn the International Space Station into a key relay for a quantum communications network.
>
> The key basis of physics underlying quantum communications is entanglement. Entangled particles are connected in a way that pretty much defies common sense. If you change the spin of one of the particles, the spin of its entangled counterpart will change – even if they’re miles apart. And that change happens nearly instantaneously – at least four orders of magnitude faster than the speed of light, according to a recent experiment.

Another remarkable aspect of this technology that sounds almost too good to be true is its potential security. After noting that quantum networks are quite fragile, the Forbes article continues:

> But why bother with these networks at

> all if they're so fragile? The answer is pretty simple – because they're almost perfectly secure. Here's how it works. Let's say that I want to send a message to New York City. My message is going to travel through normal channels, but it will be encrypted with a key. That key is transmitted via the entangled photons – so the changes I make to entangled particles on my end almost instantly show up in the particles in New York. We then compare the measurements of what I changed in my photons to those states in New York City.
>
> Those measurements then comprise an encryption key for our communications. So even if our communications are bugged, nobody can read them without knowing that encryption key. And here's the important thing: if somebody were to try to eavesdrop on the quantum entanglement, they would alter the spin of the photons. So the measurements I make and the measurements made in New York would be out of sync – thus letting us know that we have an eavesdropper. It also prevents us from creating an encryption key, so we don't send any communications. Theoretically, a quantum encrypted network is almost perfectly secure. (That said, they're not perfect, and there are some exploits.)

The announcement from the European group that they wished to carry out the experiment based on what Einstein called "spooky action over a distance" came last April. Then, in June, it was announced that China had carried out a key demonstration of concept experiment back in 2010 but waited four years to publish the result.

With China announcing progress on the technology, one would think that the West would want to accelerate its work in the area, so it would not be at all surprising if equipment for the European experiment was among the items lost

when the rocket exploded. Further, one would expect that Orbital would have been told that security for that equipment would be of the very highest level. In discussing the issue of sensitive equipment among the Antares wreckage, PCWorld this morning mentioned the incident of China perhaps examining the wreckage of the US stealth helicopter that was left behind after the mission to kill Osama bin Laden. It could well be that for this crash site, keeping the debris away from prying eyes from China is behind the call for security. Note also that the experiment quite likely would have been coordinated by the European Space Agency on behalf of the European scientists, so NASA's claim that "We didn't have any classified items on board" could be parsed as not applying to any classified items that ESA might have had on the rocket.