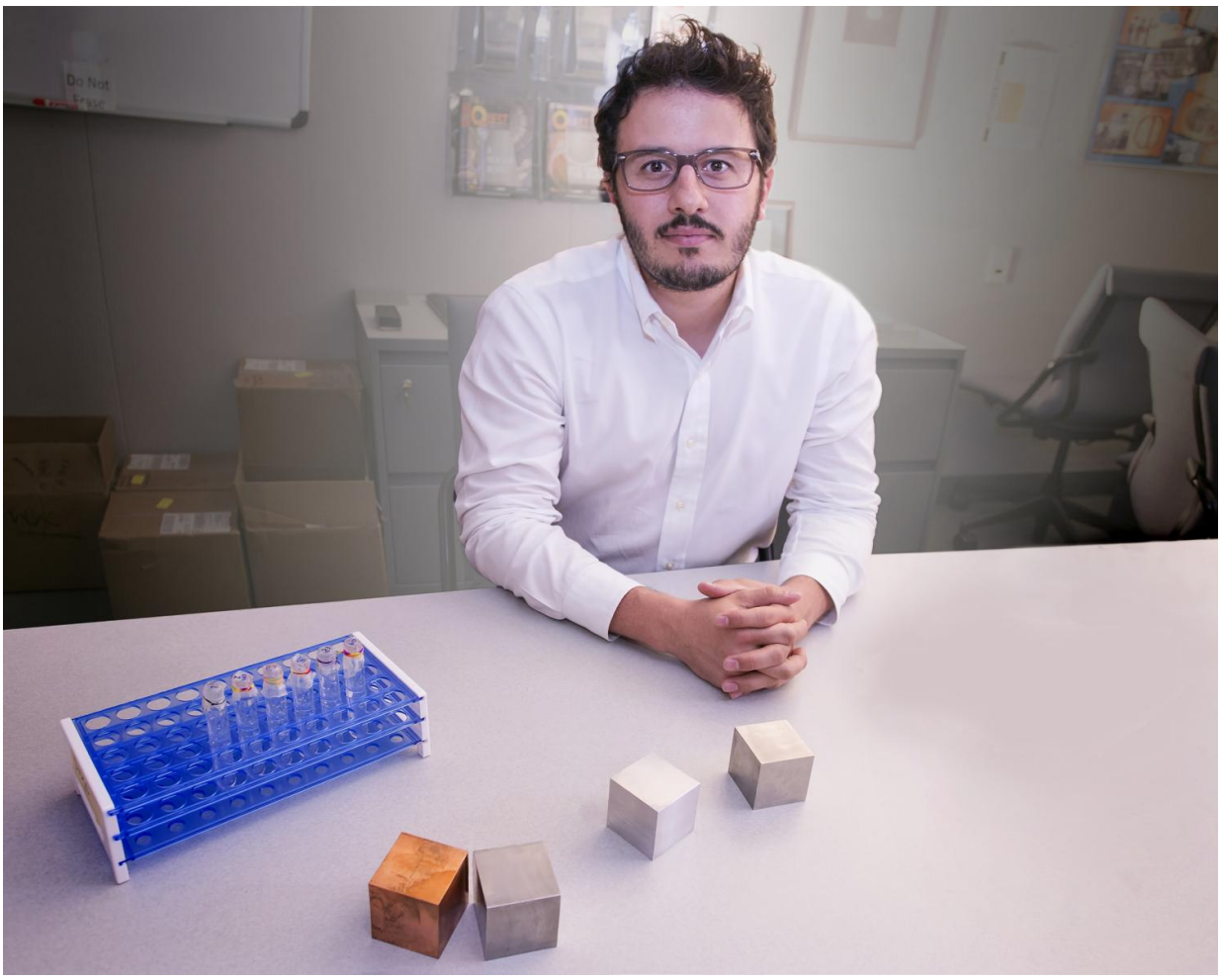
# Novel physical cryptographic technique may have applicability to future nuclear disarmament agreements

September 20 2016



Graduate student Sébastien Philippe with items used in the experiment. Credit: Elle Starkman

A system that can compare physical objects while potentially protecting sensitive information about the objects themselves has been demonstrated experimentally at the U.S. Department of Energy's (DOE) Princeton Plasma Physics Laboratory (PPPL). This work, by researchers at Princeton University and PPPL, marks an initial confirmation of the application of a powerful cryptographic technique in the physical world.

"This is the first experimental demonstration of a physical zero-knowledge proof," said Sébastien Philippe, a graduate student in the Department of Mechanical and Aerospace Engineering at Princeton University and lead author of the paper. "We have translated a major method of modern cryptography devised originally for computational tasks into use for a physical system." Cryptography is the science of disguising information.

This research, supported by funding from the DOE's National Nuclear Security Administration through the Consortium for Verification Technology, marks a promising first experimental step toward a technique that could prove useful in future disarmament agreements, pending the results of further development, testing and evaluation. While important questions remain, the technique, first proposed in a paper published in 2014 in Nature magazine, might have potential application to verify that nuclear warheads presented for disarmament were in fact true warheads. Support for this work came also from the John D. and Catherine T. MacArthur Foundation and the Carnegie Foundation of New York.

The research, outlined in a paper in *Nature Communications* on September 20, was conducted on a set of 2-inch steel and aluminum cubes arranged in different combinations. Researchers first organized the cubes into a designated "true" pattern and then into a number of "false" ones. Next, they beamed high-energy neutrons into each arrangement and recorded how many passed through to "bubble" neutron

detectors produced by Yale University, on the other side. When a neutron interacts with a "superheated" droplet in the detector, it creates a stable macroscopic bubble.

To avoid revealing information about the composition and configuration of the cubes, bubbles created in this manner were added to those already preloaded into the detectors. The preload was designed so that if a valid object were presented, the sum of the preload and the signal detected with the object present would equal the count produced by firing neutrons directly into the detectors – with no object in front of them.

The experiment found that the count for the "true" pattern equaled the sum of the preload and the object when neutrons were beamed with nothing in front of them, while the count for the significantly different "false" arrangements clearly did not.

"This was an extremely important experimental demonstration," said Robert Goldston, a fusion scientist and coauthor of the paper who is former director of PPPL and a Princeton professor of astrophysical sciences. "We had a theoretical idea and have now provided a proven practical example." Joining him as coauthors are Alex Glaser, associate professor in Princeton's Woodrow Wilson School of Public and International Affairs and the Department of Mechanical and Aerospace Engineering; and Francesco d'Errico, senior research scientist at the Yale School of Medicine and professor at the University of Pisa, Italy.

When further developed for a possible arms control application, the technique would add bubbles from irradiation of a putative warhead to those already preloaded into detectors by the warhead's owner.

If the total for the new and preloaded bubbles equaled the count produced by beaming neutrons into the detectors with nothing in front of them, the putative weapon would be verified to be a true one. But if the

total count for the preload plus warhead irradiation did not match the no-object count, the inspected weapon would be exposed as a spoof. Prior to the test, the inspector would randomly select which preloaded detectors to use with which putative warhead, and which preload to use with a warhead that was, for example, selected from the owner's active inventory.

In a sensitive measurement, such as one involving a real nuclear warhead, the proposition is that no classified data would be exposed or shared in the process, and no electronic components that might be vulnerable to tampering or snooping would be used. Even statistical noise—or random variation in neutron measurement—would convey no data. Indeed, "For the zero-knowledge property to be conserved, neither the signal nor the noise may carry information," the authors write. A necessary future step is to assess this proposition fully, and to develop and review a concept of operations in detail to determine actual viability and information sensitivity.

Important questions yet to be resolved include the details of obtaining and confirming a target warhead during the zero-knowledge measurement; specifics of establishing and maintaining the pre-loaded detectors in a way that ensures inspecting party confidence without revealing any data considered sensitive by the inspected party; and feasibility questions associated with safely deploying active interrogation measurement techniques on actual nuclear warheads in sensitive physical environments, in a way that provides confidence to both the inspected and inspecting parties.

Glaser, Goldston and Boaz Barak, a professor of computer science at Harvard University and former Princeton associate professor, first launched the concept for a zero-knowledge protocol for warhead verification in the 2014 paper in Nature magazine. That paper led Foreign Policy magazine to name the authors among its "100 Leading

Global Thinkers of 2014," and prompted other research centers to embark on similar projects. "We are happy to see this important field of research gain new momentum and create new opportunities for collaboration between national laboratories and universities," Glaser said.

**More information:** Sébastien Philippe et al. A physical zero-knowledge object-comparison system for nuclear warhead verification, *Nature Communications* (2016). DOI: 10.1038/NCOMMS12890

Provided by Princeton Plasma Physics Laboratory