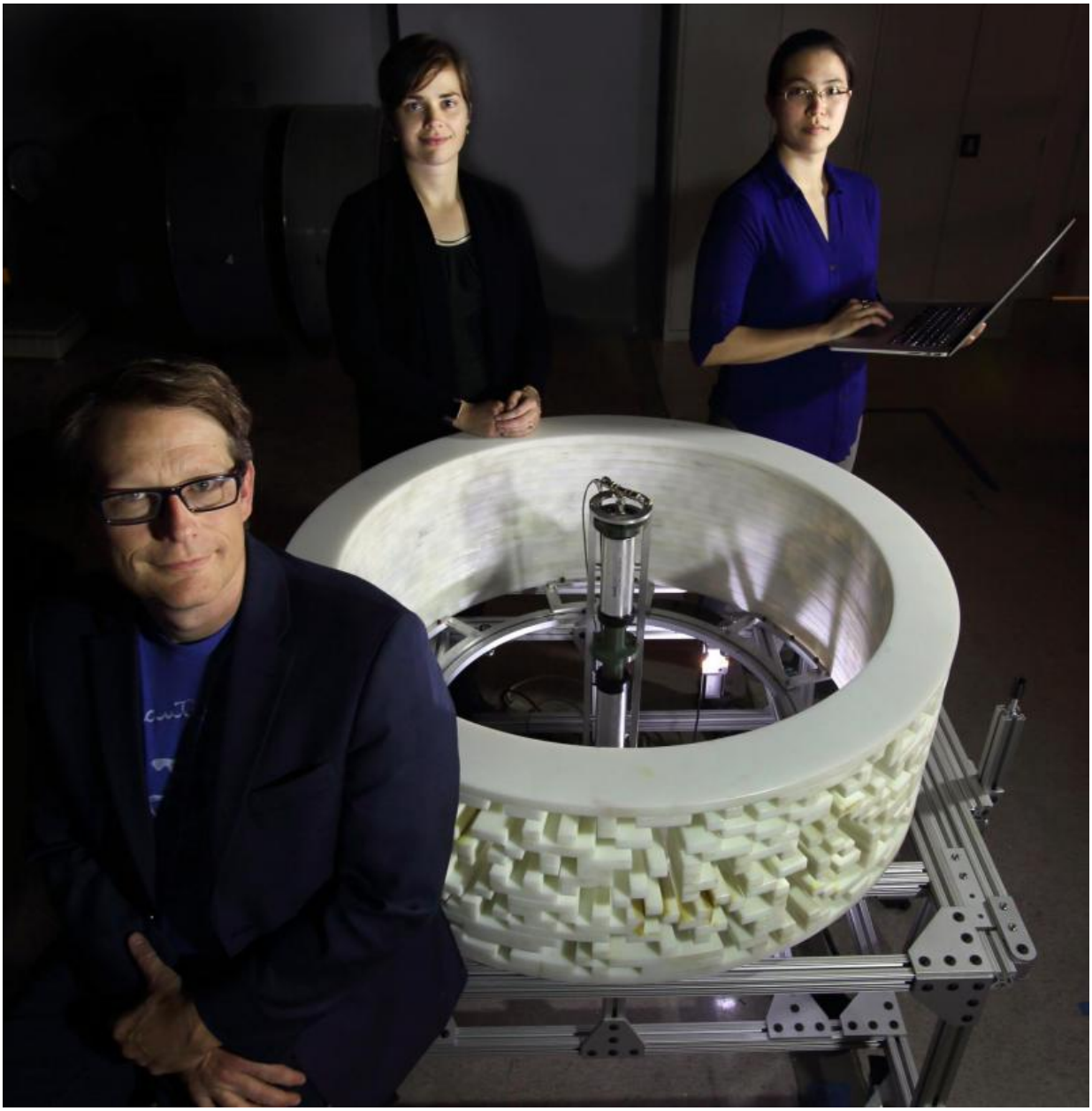
Overcoming the trust barrier in nuclear weapons verification measurements

June 6 2017



Sandia National Laboratories researchers, left to right, Peter Marleau, Patricia Schuster and Rebecca Krentz-Wee have developed a new method for verifying warhead attributes. Credit: Dino Vournas

Trust but verify. The catchphrase for arms control popularized by President Ronald Reagan sounds simple. However, verification involving sensitive data is a very complex endeavor.

Verifying that a nuclear warhead actually is a warhead may include confirming key attributes. But the act of confirming certain technical attributes might reveal critical design information—closely guarded national secrets for any country. Confirming these attributes will likely require overcoming the hurdle of protecting sensitive design data.

Sandia National Laboratories physicist Peter Marleau has developed a new method for verifying warhead attributes. Called CONFIDANTE, for CONfirmation using a Fast-neutron Imaging Detector with Anti-image Null-positive Time Encoding, the method could help address the problem of conducting verification measurements while simultaneously protecting sensitive design information. CONFIDANTE provides middle ground for the warhead owner, or host, who wants to protect sensitive information, and the monitor, who may be seeking to verify that sensitive information to confirm the inspected item is a warhead.

"CONFIDANTE is an implementation of a zero-knowledge proof (ZKP) as a way to demonstrate the validity of a claim while providing no further information beyond the claim itself," explained Marleau. "Unlike other ZKP confirmation methods, which rely on a measuring instrument that has been pre-loaded with sensitive information, CONFIDANTE allows the monitoring party to conduct the measurement in real time

without accessing sensitive design data."

Overcoming the trust barrier with ZKP

About three years ago, the Department of Energy's Princeton Plasma Physics Laboratory and Princeton University developed a ZKP object-comparison system to potentially support warhead confirmation while protecting sensitive design data. In mathematical cryptography, ZKP is accomplished by challenging a host to solve a problem that is only possible if the host possesses the information being authenticated. After repeated challenges, the host can prove it possesses that information without revealing any details about the information itself.

In the Princeton group's ZKP implementation, confirmation that an alleged warhead has the characteristics of a warhead is demonstrated through neutron transmission and emission counts measured by an array of radiation detectors. To protect sensitive design data during the measurement process, the Princeton method prepares the radiation detectors with a template rather than directly comparing in real time the images of a warhead being verified with a trusted warhead.

The template is the complement of the measurement expected from a real warhead. If the two match, they cancel each other out leaving only statistical noise, yielding no further information. The "templates" are effectively destroyed by the measurement, so the monitor does not have the opportunity to maintain the data to which a measurement is compared.

"But to protect the sensitive design data, the template, the process of pre-loading it, and the detector itself, will be off limits to the monitoring party," said Marleau. "All of this, including the actual measurement must be conducted by the host. When the monitoring party loses control of so much of the measurement process, it becomes difficult to trust its

authenticity."

Monitor-controlled, real-time authentication

Marleau, his colleague Patricia Schuster, a University of Michigan postdoctoral fellow, and Rebecca Krentz-Wee, a University of California, Berkeley, nuclear engineering graduate student, set out to solve this problem. "We asked ourselves, is there a method that maintains the nice property of a positive match indicated only by statistical noise while allowing a monitoring party to be in control of the detector during the entire measurement process?" said Marleau.

They explored different concepts that might provide more practical and verifiable ZKP implementations. One promising solution is time-encoded imaging (TEI), a method Sandia developed over the past five years with funding from the National Nuclear Security Administration's Defense Nuclear Nonproliferation Research and Development program, based on earlier research funded by the Laboratory Directed Research and Development program.

TEI is a new approach for indirect detection and localization of special nuclear materials, which relies on encoding directional information in the time-dependent modulation of fast neutron detection rates. Sandia developed TEI to overcome the precise calibration and high cost of typical detection, which uses arrays of detectors.

TEI uses a single detector within a cylindrical coded mask. As the mask rotates, radiation from the object is modulated by a pattern of apertures and mask elements on the cylinder. Using TEI, a single detector can do the work of multiple detectors in creating an entire two-dimensional image of the object.

"We realized that if we designed the mask such that the pattern on one

half of the cylinder is the inverse of the other half, an object on one side of the system will project the inverse image of an object on the opposite side of the system at all times if and only if the two objects are identical. The image and anti-image will effectively cancel each other out and the detector will show a constant unmodulated rate," said Marleau. "And we can do it without ever recording potentially sensitive information."

Because no information other than statistical noise is stored or recorded in the detector—unlike a template approach—the host party in theory can certify that no sensitive information is at risk. The monitor then can have full access to the data in real time, potentially even conducting the measurement themselves. Using this method, two objects can be confirmed as identical. To prove in addition that that they are warheads, both negotiating parties would need to agree on an authentic warhead—a "golden" warhead to be compared to any other object measured. This authenticity then transfers to all objects that have been or ever will be measured.

Extra layer of protection

One possible glitch is that if the two objects aren't aligned perfectly, the measurement could reveal spatial information. "A slight misalignment could reveal outlines," said Marleau.

For the verification measurement, the monitoring party only needs to confirm that the detector is measuring a constant rate consistent with statistical noise.

"You can define specific metrics that can be updated in real time and can tell the monitoring party if the data is consistent with counting statistics," said Marleau.

Distilling the data into a single number is also irreversible—meaning

there is no way to reverse engineer the data to learn design characteristics of the warhead being verified even if something happened, such as accidental misalignment, that produced a false negative result.

First proof-of-concept

The Department of State, Bureau of Arms Control Verification and Compliance (AVC) through the Key Verification Assets Fund funded Sandia to perform a proof-of-concept measurement. CONFIDANTE was tested at Lawrence Livermore National Laboratory using identical plutonium dioxide hemispheres. "We knew these two objects were identical going into the test," said Marleau. "CONFIDANTE confirmed this with unmodulated counting statistics. We also did a successful negative test showing that two different objects did not cancel each other out."

This test demonstrated feasibility so now the Sandia team plans to improve CONFIDANTE with a more compact gamma ray version of the imager. Marleau also hopes to perform another feasibility test at the Pantex Plant, a Department of Energy facility for assembly and disassembly of nuclear weapons.

"It's critical that we continue to develop and operationally evaluate CONFIDANTE and other warhead authentication methods," said Marleau. "These tools need to be ready to go before there is an exercise or a treaty being negotiated. At that point, there is little time for research and development. I believe CONFIDANTE has the potential to open new possibilities in treaty verification. With technical solutions in place, parties may be more willing to engage in negotiations."

Provided by Sandia National Laboratories