Researchers develop a 'physical cryptography' for secure and accurate accounting of the world's nuclear arsenals

July 20 2016, by Meg Murphy

"It is easier to make a replacement nuclear weapon from scratch than to try to pass off a fake object as a weapon," says R. Scott Kemp in MIT's Department of Nuclear Science and Engineering about a new method to verify that a country's claimed warheads are authentic without disclosing classified information. Credit: Lillie Paquette/School of Enginering

Verifiably reducing the number of nuclear weapons in the world will require more than international diplomacy; a scientific breakthrough is needed. To date, all nuclear arms control treaties have been limited in a peculiar way: Participants cannot determine that the warheads of other countries being counted are real.

Now researchers led by R. Scott Kemp in MIT's Department of Nuclear Science and Engineering say they have found an answer. Their method involves nuclear resonance fluorescence, a new form of single-pixel tomography, and careful attention to the information content of physical processes. The proposed solution marks a major advance in a search for a workable method that has been ongoing since 1963.

At the heart of the matter is the protection of classified information; states do not want foreign inspectors gaining access to the secret details of their nuclear-weapon designs. To avoid this, states have refused to allow inspections that would confirm the authenticity of claimed warheads—and for good reason: Previous review techniques would have put national secrets at risk or failed to detect even very simple cheating.

Finding a solution to this quandary is essential to continuing the improvements in global security that began at the end of the Cold War. For example, the United States and Russia signed the New Strategic Arms Reduction Treaty in 2010, committing both countries to a cap of 1,550 deployed nuclear warheads each by February 2018. Yet there are no provisions to monitor the thousands of weapons that will be removed from deployment to satisfy the treaty, and thus no way for one side to know whether the other side's weapons are being stored for later use, destroyed, or even sold on the black market.

The solution proposed depends, in part, on nuclear resonance florescence, a process whereby a photon can be absorbed by an atom's nucleus. If a warhead owner attempts to replace the valuable plutonium

parts of the weapon with a surrogate material, that substitution will be detected because every material exhibits a different nuclear-absorption behavior. The system can also determine if any geometric changes to the warhead have been made, or if pieces of the warhead have gone missing.

The new findings are detailed today in Proceedings of the National Academy of Sciences in a paper entitled, "Physical Cryptographic Verification of Nuclear Warheads," by Kemp, MIT professors Areg Danagoulian and Ruaridh R. Macdonald, and PhD student Jayson R. Vavrek. Using a simulated Soviet warhead from the 1989 Black Sea experiments, the authors demonstrated that a pair of 21-second measurements can spot a set of canonical hoax warheads with a probability greater than 99.9 percent.

"What really sets our method apart is the extent to which we can rule out cheating scenarios," says Kemp, the Norman C. Rasmussen Career Development Professor of Nuclear Science and Engineering. "We mathematically define the space of all theoretical objects that could spoof the system into thinking it was measuring a real warhead. We then designed a protocol that reduced the space to a subset of objects that are more difficult to manufacture than a real warhead. In other words, it is easier to make a replacement nuclear weapon from scratch than to try to pass off a fake object as a weapon."

Peter Fisher, head of the Department of Physics at MIT and a top nuclear security consultant with the federal government, said the research will prove useful on many levels. "This is an important new method for verifying a nuclear warhead's type and condition without the operator knowing anything technical about the warhead itself," he said. "Separate from that, the mathematical underpinnings of Scott's method have a wide range of applicability," says Fisher, who was not involved with this particular MIT project.

James M. Acton, senior associate at the Carnegie Endowment for International Peace and co-director of the endowment's Nuclear Policy Program, says he hopes the new paper might open up future treaty opportunities. Acton—who specializes in deterrence, disarmament, and nonproliferation—adds the current state of U.S.-Russian politics leaves no prospect of a new arms control treaty in the near future, but he is hopeful there will be another in due course. At that point, he says, we will need a means of verifying that claimed warheads are authentic without disclosing classified information. "To date, arms control has got no further than requiring warheads to be removed from delivery vehicles, but such warheads can be placed in storage rather than destroyed," he notes.

Many competing techniques rely on electronics to protect classified information, but experts do not fully trust electronics, as they may secretly record information or have hidden functionality, and they are prone to hacks and side-channel exploits. "Our technique achieves the same goal with the physics intrinsic to the process: You can't hack the laws of nature," says Danagoulian, an assistant professor of nuclear science and engineering, who co-led the project. "Our hope is that Russian scientists will assimilate these ideas and, after thorough scrutiny, will agree to work together using this general framework."

Ken Jarman, senior scientist at Pacific Northwest National Laboratory, who studies different warhead verification concepts, visited MIT this summer to learn more about the research and discuss specific findings with Kemp and Macdonald. Jarman says the team's approach is distinctive and holds potential. "One of the things that is best about what MIT is doing is that the team is really pushing forward rigorous analysis of key things: completeness, soundness, and information protection."

In terms of next steps, the researchers plan to build an experimental demonstration and do further studies on the information security of the

technique under different real-world scenarios. Although there is much to do at MIT, the researchers say an increased collaboration with the national labs and other universities will be essential in turning the concept into a practical and internationally approved system.

More information: R. Scott Kemp et al. Physical cryptographic verification of nuclear warheads, *Proceedings of the National Academy of Sciences* (2016). DOI: 10.1073/pnas.1603916113

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology