Physical cryptographic verification of nuclear warheads

R. Scott Kemp, Areg Danagoulian, Ruaridh R. Macdonald, and Jayson R. Vavrek

How does one prove a claim about a highly sensitive object such as a nuclear weapon without revealing information about the object? This paradox has challenged nuclear arms control for more than five decades. We present a mechanism in the form of an interactive proof system that can validate the structure and composition of an object, such as a nuclear warhead, to arbitrary precision without revealing either its structure or composition. We introduce a tomographic method that simultaneously resolves both the geometric and isotopic makeup of an object. We also introduce a method of protecting information using a provably secure cryptographic hash that does not rely on electronics or software. These techniques, when combined with a suitable protocol, constitute an interactive proof system that could reject hoax items and clear authentic warheads with excellent sensitivity in reasonably short measurement times.

Kemp et al, PNAS (2016) 201603916. All rights reserved by Elsevier.
Reproduced for educational purposes only.

Motivating background

Start with something that everyone in your audience cares about. The background should provide context for your problem or knowledge gap.

Problem statement or knowledge gap

What central question are you trying to answer? Focus in on the specific need that your research addresses; this is the primary motivation for your work.

"Here we show…"

State what you specifically did to solve the problem. Example statements might include: "We simulated/measured XYZ…"

Results

Briefly summarize your main results or conclusions that address the problem statement or knowledge gap. You can include key data but save the fine details for the main document.

Implications

Explicitly state the implications of your findings by linking back to the motivating background. What impact do your findings have on this area of research? Try to answer "so what?" and "now what" questions.