Physical cryptographic verification of nuclear warheads

R. Scott Kemp[a,1,2], Areg Danagoulian[a,1], Ruaridh R. Macdonald[a,1], and Jayson R. Vavrek[a,1]

[a]Laboratory for Nuclear Security and Policy, Massachusetts Institute of Technology, Cambridge, MA 02139

Kemp, et. al. PNAS (2016)
doi: 10.1073/pnas.1603916113

Overall summary and importance statement

Defining the scope of the problem considered

Trends in nuclear disarmament indicate a need for a provably sound, complete, and information-secure method for authenticating nuclear warheads. The system proposed here seeks to meet these requirements with a mathematically quantifiable physical framework and logically sound set of axioms. By the virtue of being in the public domain, various aspects of the system can be freely studied and scrutinized by any participant in the arms reduction process. In addition to theoretical considerations, there may be important operational limitations to implementing such a system in existing national-security environments, which will require further study by government experts.

Soundness against strategically meaningful hoax warheads is achieved by careful attention to the logical connections that link observables to conclusions about warhead authenticity; by exploiting a process in nuclear physics that acts as a naturally occurring one-to-one function between energy and isotope identity; and through the introduction of a single-pixel tomographic transform that provides a unique measure of the warhead's geometry. Information is protected by the intrinsic physics of the system rather than relying on difficult-to-certify electronic circuits or software. Although electronics are used to operate the detectors and to measure signals leaving the shielded area, no sensitive information ever becomes experimentally observable.

Simulations for a bremsstrahlung-based system using available technologies and the simulated geometries suggest that two 21-s measurements should be able to reject a canonical set of hoaxes with greater than 99.9% probability, while falsely alarming on an authentic warhead about once in every 10,000 warheads. Realistic foil and warhead geometries will almost certainly require somewhat longer measurements than those simulated. Work remains to validate these simulations in an experimental setting. NRF cross-section data for some isotopes, mainly those not used here, are still sparse and may need to be measured if those isotopes are to be included in the verification process.

If a bremsstrahlung beam is used, several information security questions remain open. The information content of the continuum underneath the NRF signal is at present poorly understood; the simultaneous observation of multiple NRF transitions, which is unavoidable with bremsstrahlung, will require careful study of countermeasures to ensure the system remains underconstrained; and dose to the warhead will be high when using bremsstrahlung. Many of these problems can be avoided by using a tunable monochromatic photon source.

Finally, although the example system suggests excellent performance for canonical hoaxes and measurements on the order of minutes, a relationship between measurement time and the upper bound on the probability of failing to reject any possible hoax would be a useful future development. As these probabilities are inherently a function of hoax geometry, such a statement requires a description of the space of all possible hoax objects, which might first require the development of an inversion formula for the $\mathcal{K}$ transform. This remains as future work.

Engineering and physics considerations that make this solution unique

Importance statement about engineering solution

Statement of specific results

Identification of future data necessary for implementable system

Limitations on a proposed extension identified

Potential solution to identified limitation

Work to be continued in the future