Princeton Zero-Knowledge Warhead Verification Project

Sébastien Philippe,[1] Alexander Glaser,[1] Boaz Barak,[2] and Robert J. Goldston[1,3]
[1]Princeton University, [2]Microsoft Research, [3]Princeton Plasma Physics Laboratory

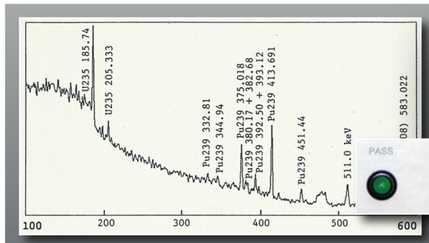
Abstract

Verification of future nuclear arms control agreements could require the independent authentication of possibly thousands of nuclear warheads or warhead components currently in storage or awaiting dismantlement. To address this challenge, we propose an approach to nuclear warhead authentication envisioning a template-match *zero-knowledge protocol* using active neutron measurement techniques and non-electronic detectors.

Zero-knowledge protocols are interactive proof systems that have the powerful property of yielding no knowledge beyond the validity of an assertion. As opposed to most cryptographic concepts, Goldwasser, Micalli and Rackoff invented the idea of zero-knowledge proofs in the late 1980's for applications in the digital world; we translate it for the first time for a non-trivial physical application.

Under the proposed *physical* zero-knowledge protocol, the host country, *prover*, can convince with high probability an inspector, *verifier*, that a nuclear weapons is authentic without revealing anything about it including information considered highly *sensitive*. Timely demonstration of the viability of such an approach could be critical for the next round of arms-control negotiations.

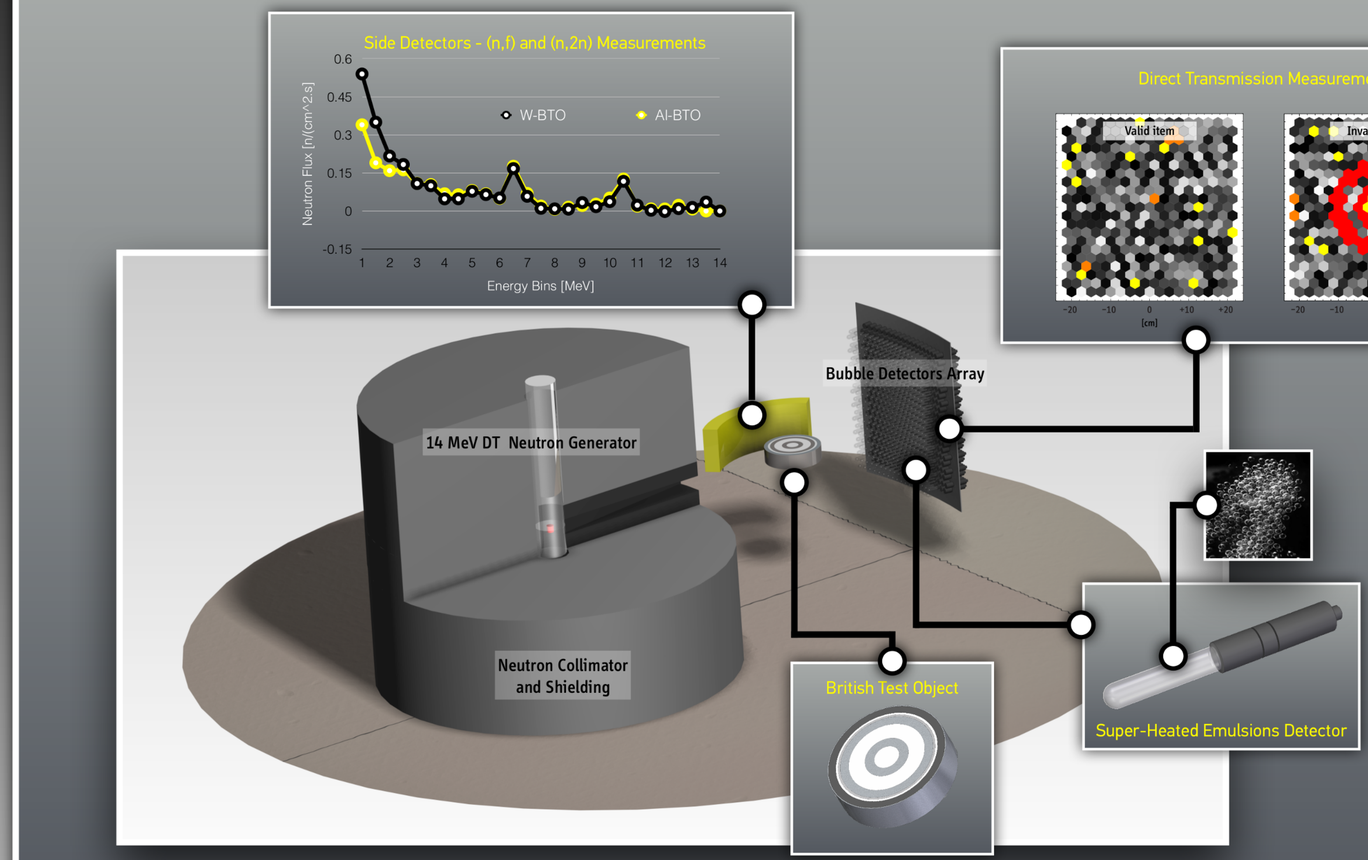
The Challenges of Authentication



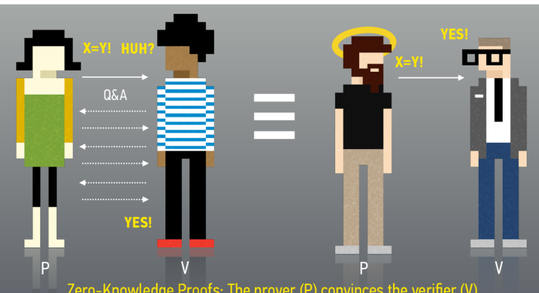
Sources: Left, Black Sea Experiment. Top-right, DOE. Bottom-right, UK-Norway Initiative.

Nuclear weapons have unique signatures but most of them are sensitive and cannot be revealed to inspectors. Electronic equipment has been used to "filter" classified information but it is difficult to certify and authenticate. For example, inspectors may not be allowed to examine the measurement equipment after the inspection finishes.

The Experimental Set-Up



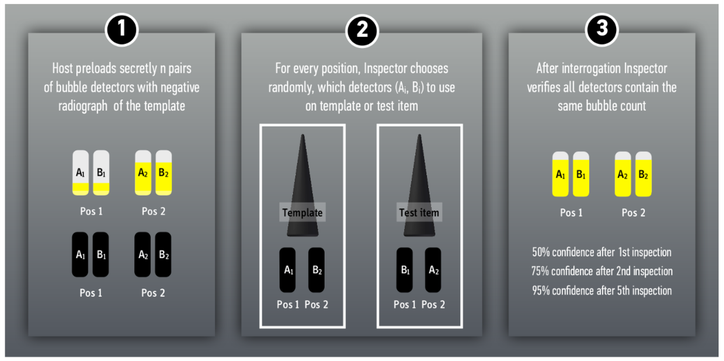
Zero-Knowledge Interactive Proofs



Zero-Knowledge Proofs: The prover (P) convinces the verifier (V) that s/he knows a secret without giving anything about the secret itself away

Adapted from O. Goldreich, "Foundations of Cryptography, Volume 1: Basic Techniques,"Cambridge University Press, 2001

The Inspection Protocol



More to Explore - References

A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature*, 510, 26 June 2014, 497–502
B. Richard Stone, "Not-seeing is Believing," *Science*, 344 (6191), 27 June 2014, 1436–1437
C. S. Goldwasser, S. Micali, and C. Rackoff, The Knowledge Complexity of Interactive Proof-Systems, SIAM Journal on Computing, 18 (1), pp. 186-208, February 1989.
D. S. Philippe, A. Glaser, M. Walker, B. Barak and R. J. Goldston, Resolving the Information Barrier Dilemma: Next Steps Towards Trusted Zero-Knowledge Nuclear Warhead Verification, INMM Information Analysis Technologies Conference, 12-14 May 2014, Portland, Oregon.
E. R. J. Goldston, F. d'Errico, A. di Fulvio, A. Glaser, S. Philippe and M. Walker, Zero-Knowledge Warhead Verification: System Requirements and Detector Technology, 55th Annual INMM Meeting, 20-24 July 2014, Atlanta, Georgia.
F. M. Kütt , S. Philippe, B. Barak, A. Glaser and R. J. Goldston, Authenticating Nuclear Warheads With High Confidence, 55th Annual INMM Meeting, 20-24 July 2014, Atlanta, Georgia.
G. B. Fisch, D. Freund, and M. Naor, Physical Zero-knowledge Proofs of Physical Properties, Advances of Cryptology — CRYPTO 2014, Springer Berlin, 313—336, 2014.