
© Paul Schambroom

How I Learned to Stop Worrying and Dismantle the Bomb

A New Approach to Nuclear Warhead Verification

Alexander Glaser

Department of Mechanical and Aerospace Engineering
and Woodrow Wilson School of Public and International Affairs
Princeton University

Princeton Research Symposium
November 17, 2012

Revision 5

7 779 194 804 244 557

is not a prime number

23 985 737 x 324 325 861 = 7 779 194 804 244 557

Can one prove that a number is not a prime
without revealing its factors?

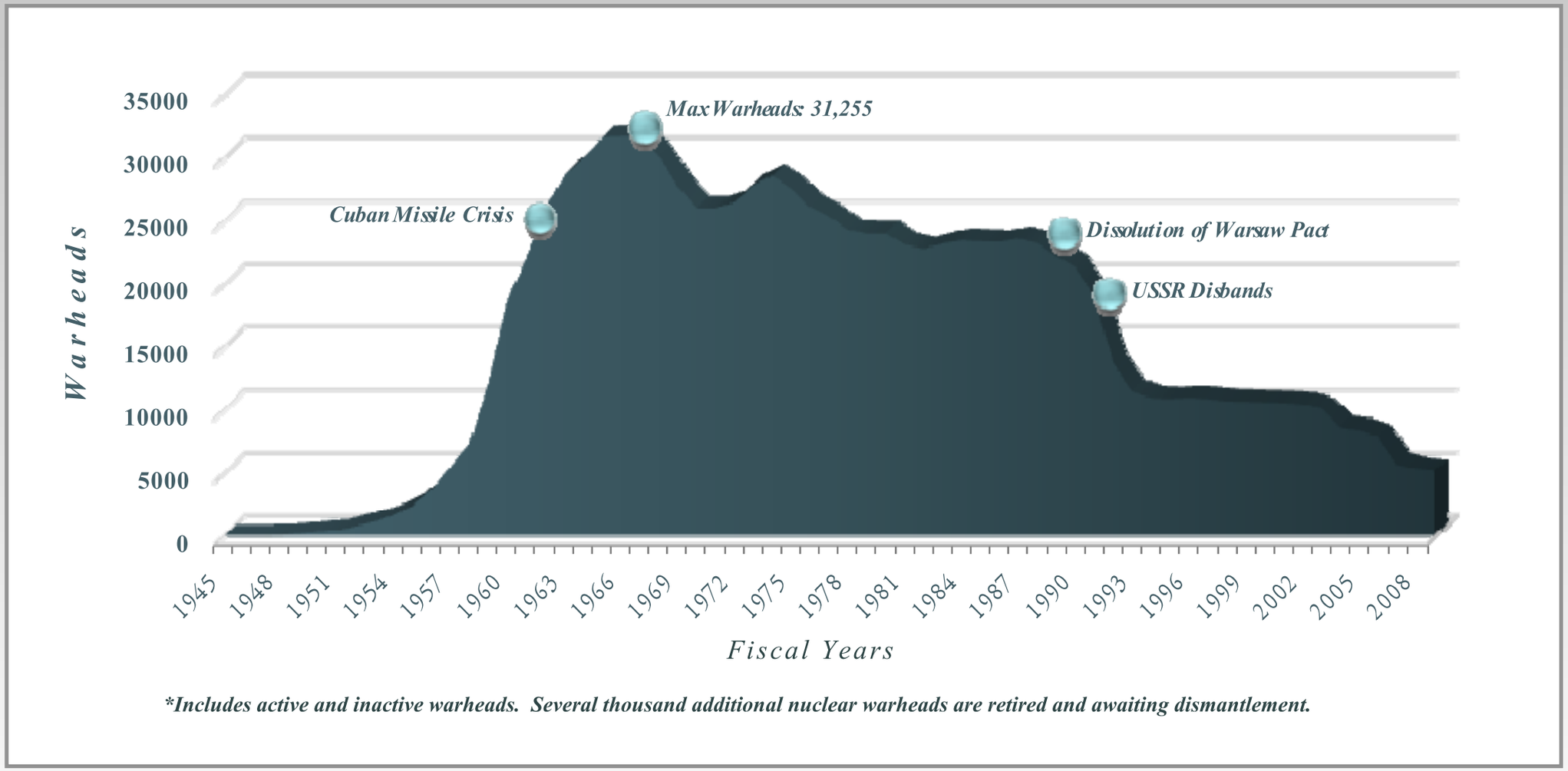
Background

Nuclear Weapons After the Cold War and the Challenge of Verifying Nuclear Disarmament

U.S. Nuclear Weapons Stockpile, 1945–2009

5,113 warheads in (active and inactive) stockpile, as of September 2009

including 1,665 operationally deployed strategic warheads, as of September 2011
(but not including about 4,000 retired warheads in storage and awaiting dismantlement)



*Includes active and inactive warheads. Several thousand additional nuclear warheads are retired and awaiting dismantlement.

Increasing Transparency in the U.S. Nuclear Weapons Stockpile, Fact Sheet, U.S. Department of Defense, Washington, DC, 3 May 2010

Thousands of Nuclear Weapons Are No Longer Deployed and Currently In Storage

B-61 thermonuclear bombs in storage
Maximum yield: 340 kt(TNT); more than 3,000 made
Source: www.usafnukes.com

Components of a B-61 nuclear bomb
Source: U.S. Department of Energy

How Can the Inspecting Party Be Assured That a Genuine Warhead is Being Offered for Dismantlement?

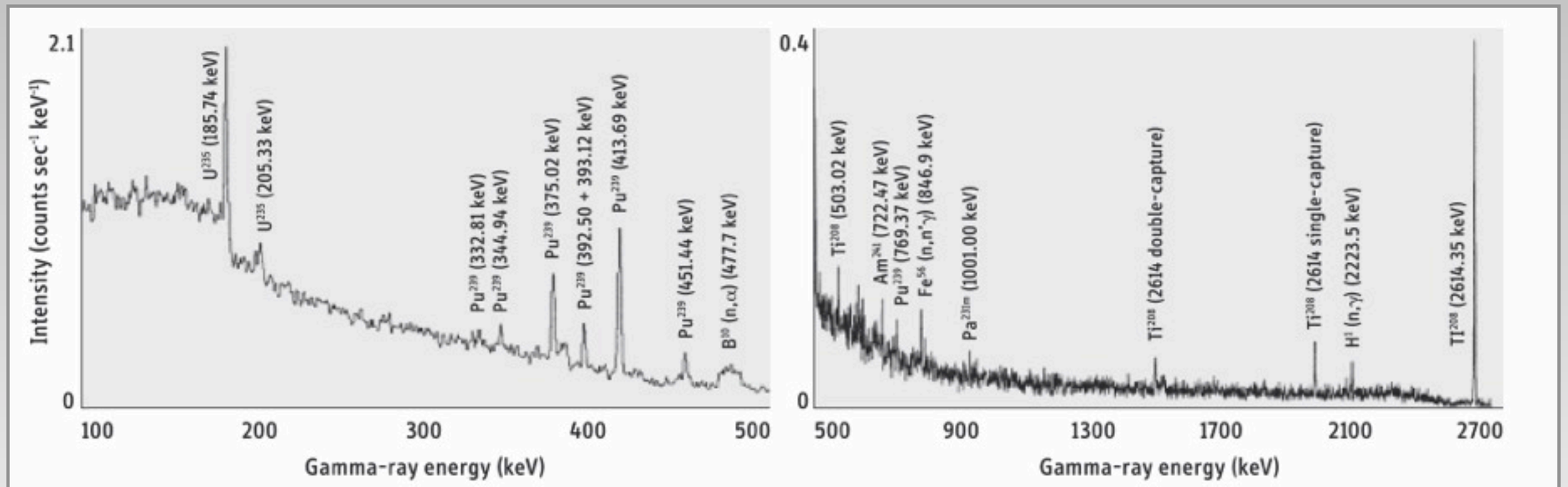
Hypothetical scenarios that a country "hedging its bets" might consider

Present objects that are similar to genuine warheads
except that some fissile material has been substituted (e.g. with natural uranium)
Objective: Withhold fissile material

Present objects that might or might not resemble real warheads
(but presumably contain some fissile material)
Objective: Withhold real warheads

Nuclear Warheads Have Unique Signatures

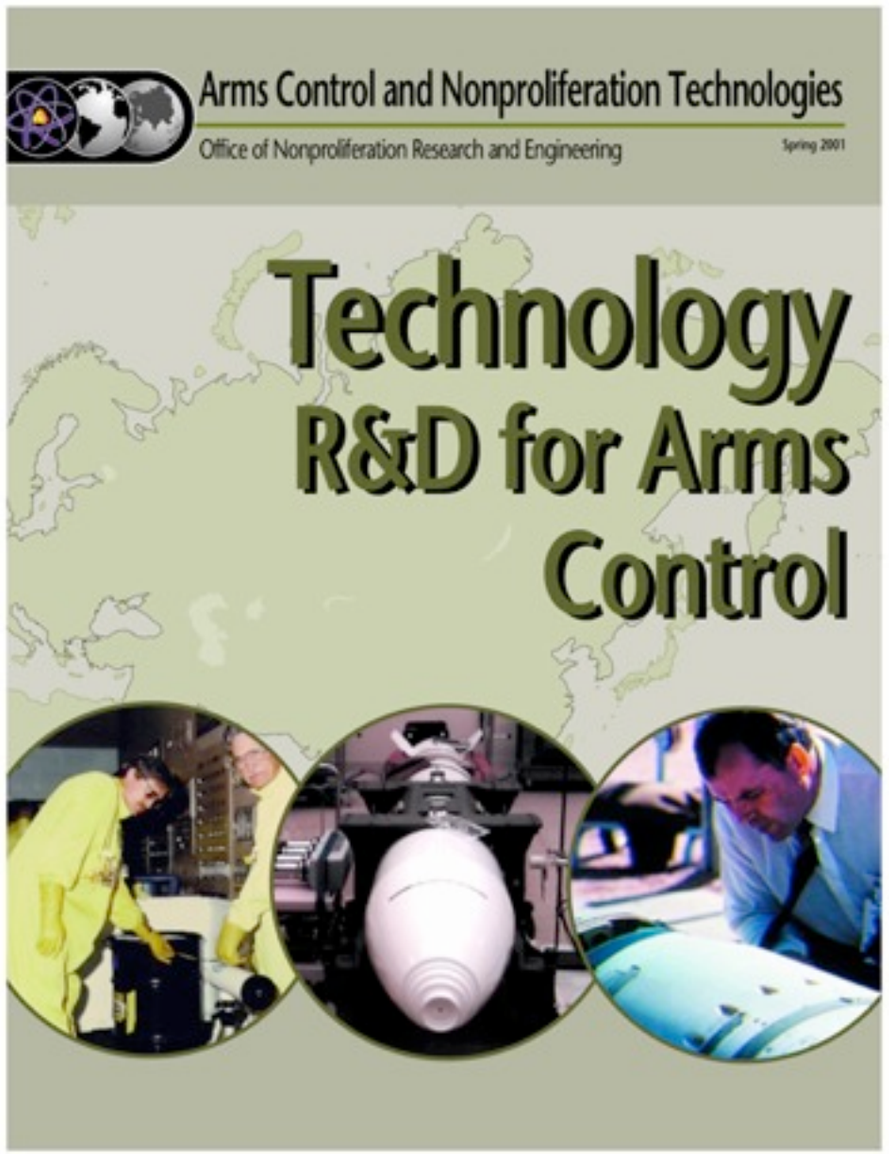
(but most of them are sensitive and cannot be revealed)



Gamma radiation spectrum from a Soviet warhead measured in 1989

Steve Fetter, Thomas B. Cochran, Lee Grodzins, Harvey L. Lynch and Martin S. Zucker
"Measurements of Gamma Rays from a Soviet Cruise Missile," *Science*, Vol. 248, 18 May 1990, pp. 828–834

Inspection Systems for Nuclear Warhead Verification Have Been Under Development Since the 1990s



edited by David Spears, 2001

Attribute Approach

Confirming selected characteristics of an object
in classified form
(for example the mass of plutonium)

Template Approach

Comparing the radiation signature
from the inspected item with a reference item
("golden warhead") of the same type

Information Barrier

Technologies and procedures that prevent the
release of sensitive nuclear information
(needed for both approaches)

"After all these years, no one has yet demonstrated either an attribute or template type system using a classified test object in such a way that specialists from the inspecting country can then thoroughly examine and proof the measurement equipment."

James Fuller, October 2012

Princeton Verification Project

in Partnership with Global Zero

Princeton Verification Project

in collaboration with Rob Goldston and Charles Gentile, PPPL and Boaz Barak, Microsoft Research New England

TEMPLATE APPROACH

- Use 14.1-MeV neutron source ($1.5\ 10^8$ n/s) available at PPPL
- Use unclassified test objects that do not contain fissile materials (tantalum, lead, depleted uranium, …)
- Avoid or minimize role/use of information barriers
- Validate conceptual approach with simulated data

Project currently funded by Global Zero (www.globalzero.org) and U.S. Department of State and supported by PPPL Proposal Development Funds

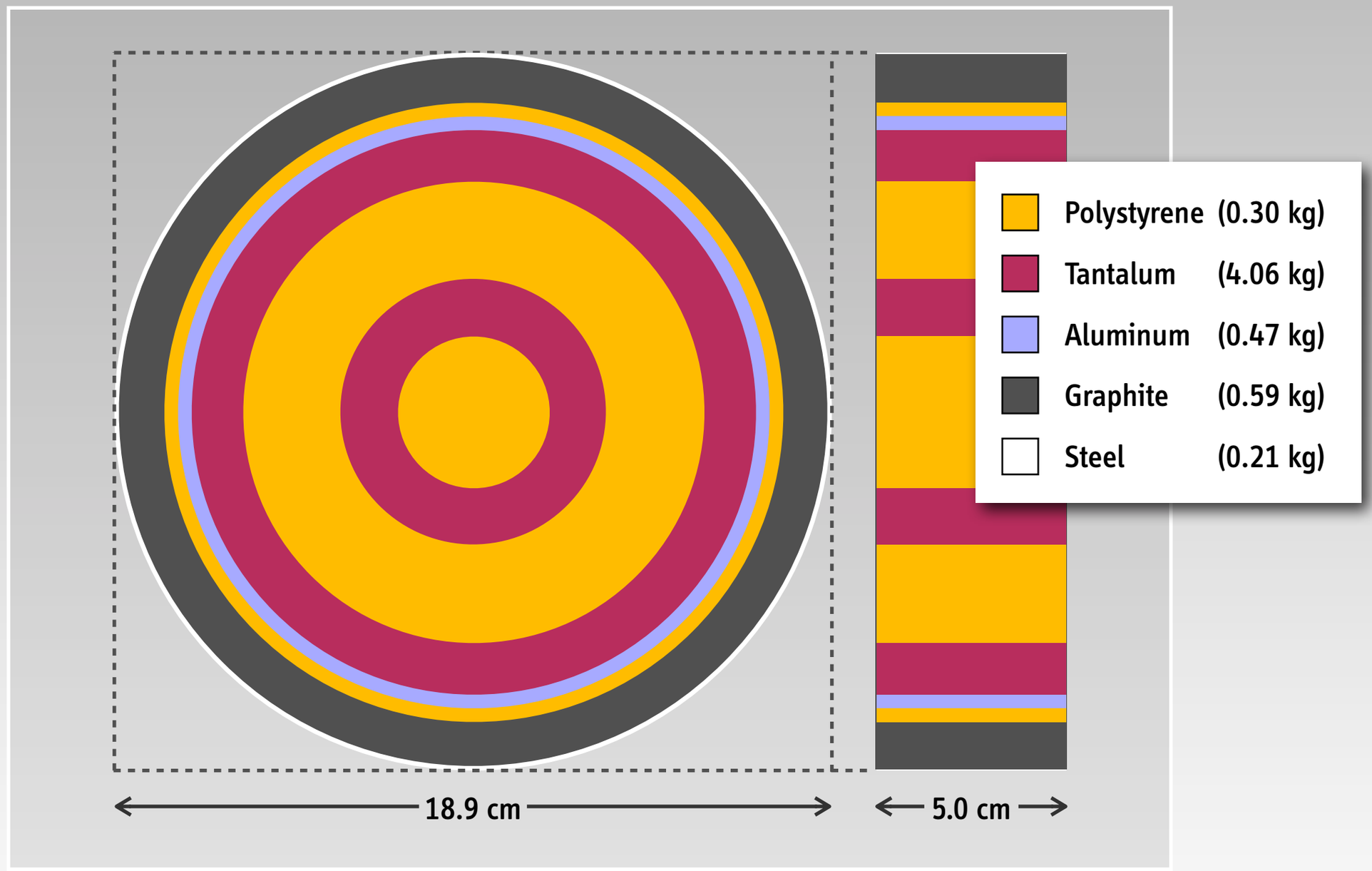
What We Don't Use

(and Don't Need for Our Proof-of-concept)

Mockup of a MK-12 Reentry Vehicle with a W62 warhead

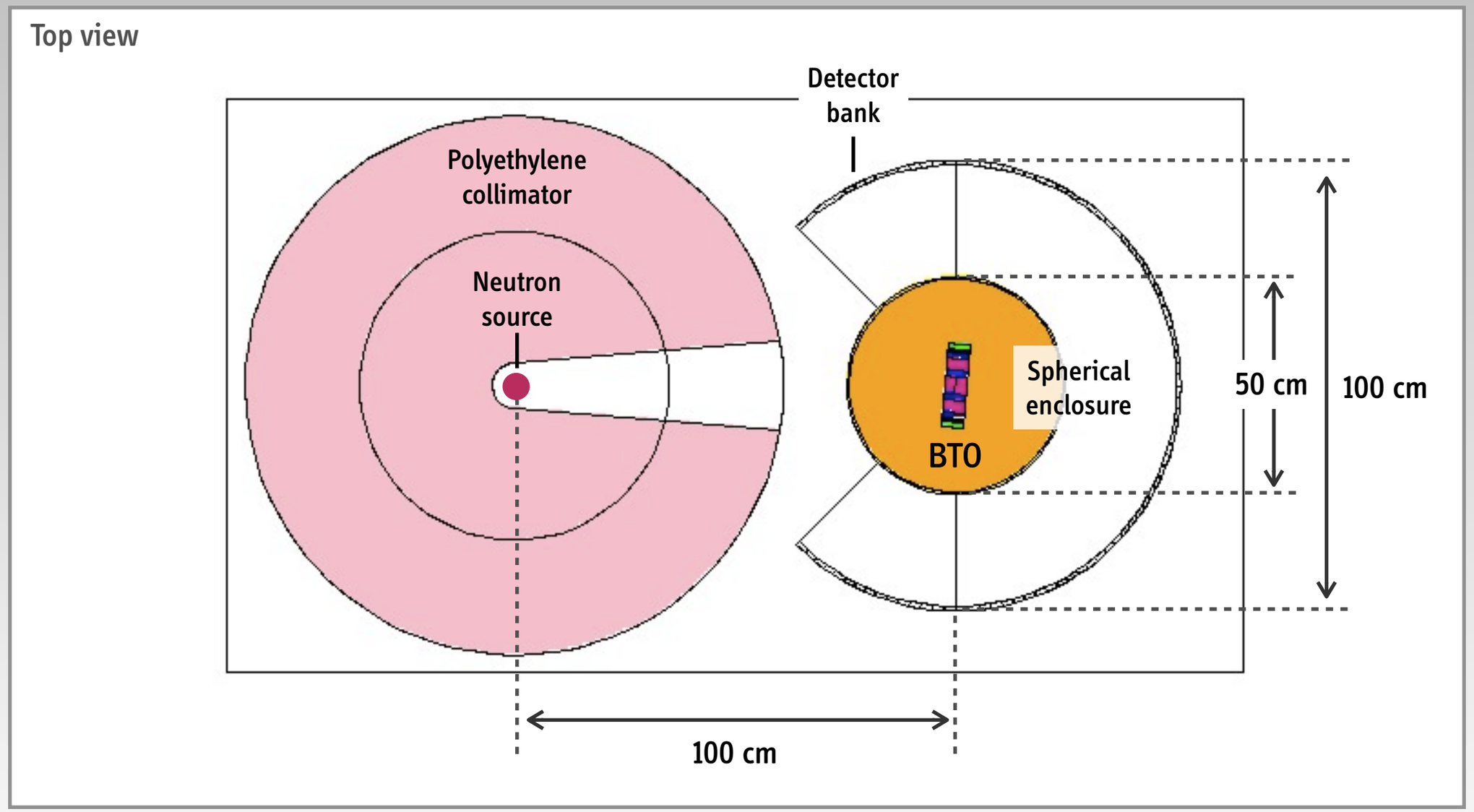
(Note: the final W62 was dismantled in August 2010, www.energy.gov/articles/dismantling-history-final-w62-warhead)

“British Test Object”



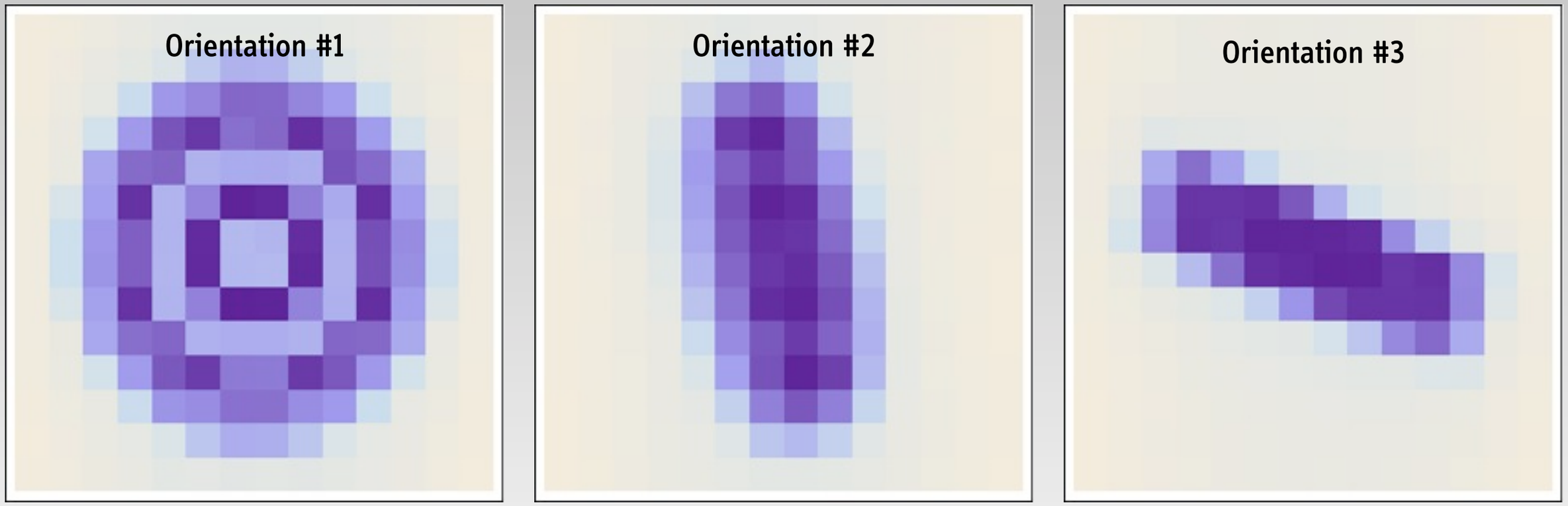
James Hall, “Uncovering Hidden Defects with Neutrons,” *Science & Technology Review*, May 2001, www.llnl.gov/str/May01/Hall.html

Experimental Setup



Radiograph of Test Item in Container

Simulated data, MCNP5 simulations with 10 billion source neutrons



How Do We Prevent Sensitive Information from Being Detected?

We Avoid Detector-Side Electronics

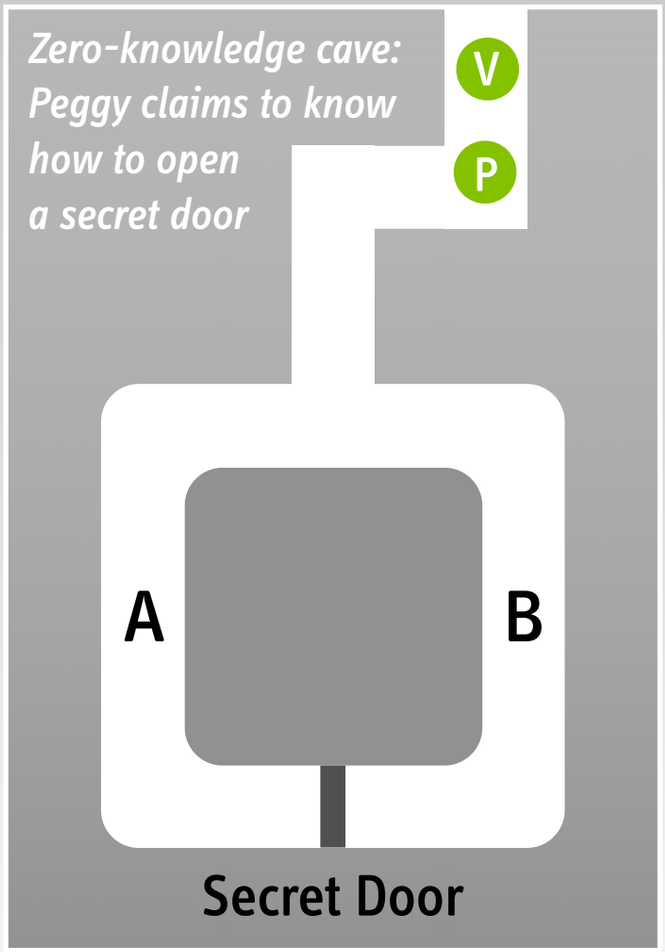
Superheated drop (or “bubble”) detectors

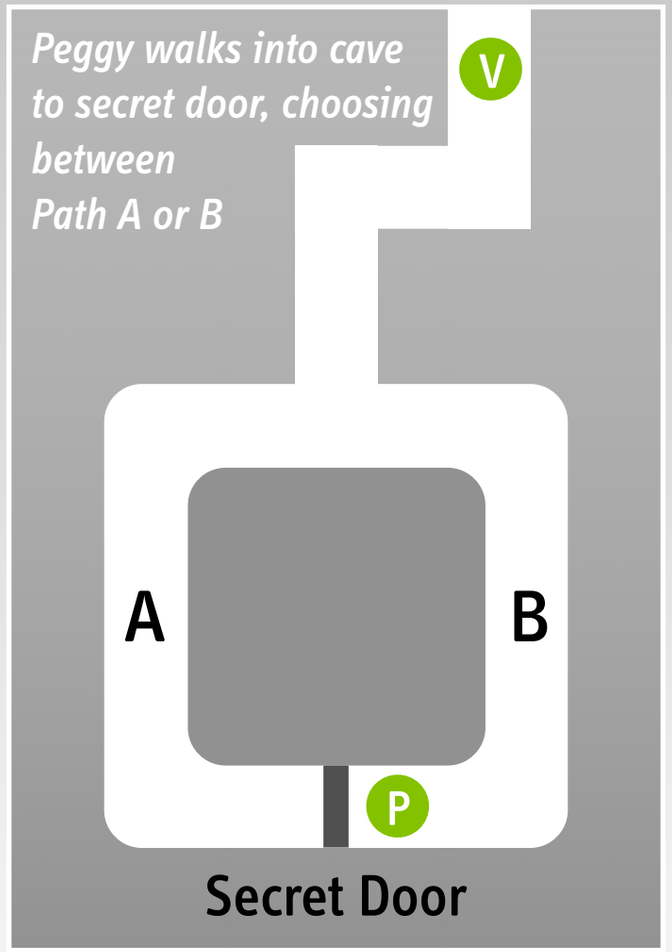
Detectors with different neutron-energy thresholds are available

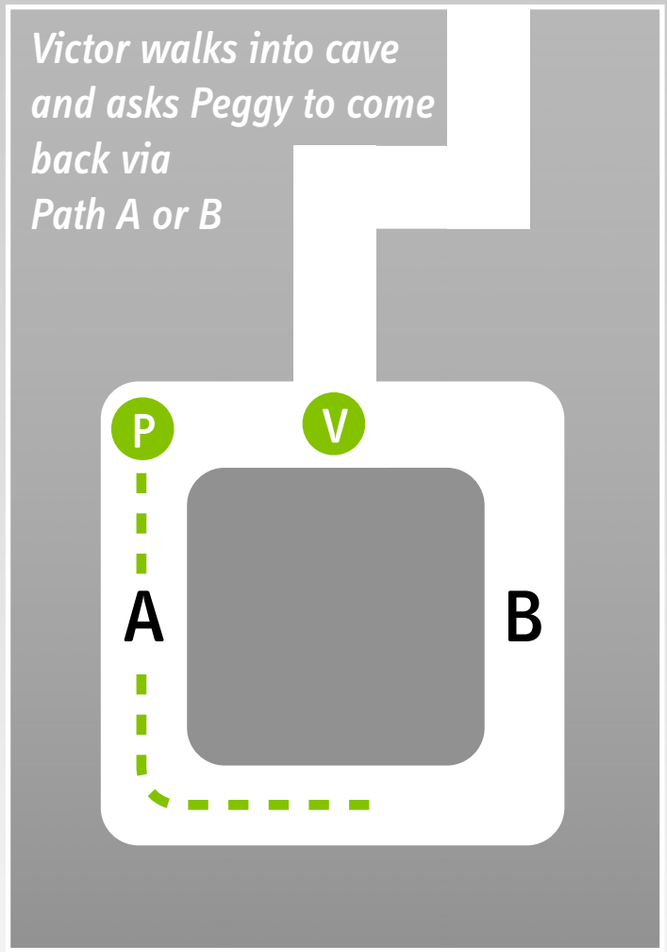
(no cutoff, 500 keV, 1 MeV, 10 MeV)

We Use a Zero-Knowledge Protocol

Zero-Knowledge Proofs: Peggy (P) proves to Victor (V) that she knows a secret without giving anything about the secret itself away





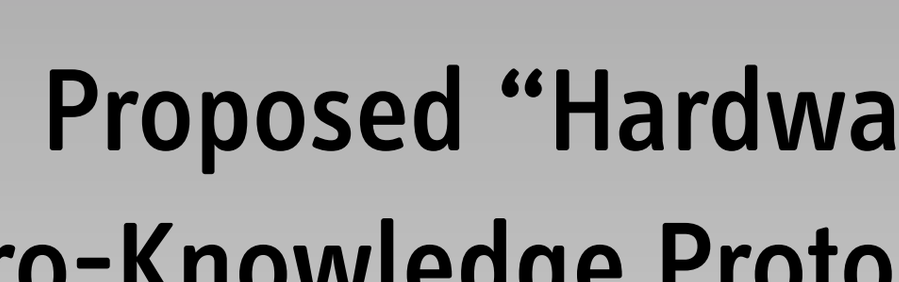


Proposed “Hardware Implementation” of a Zero-Knowledge Protocol for Warhead Verification

After every measurement, each bubble detector has “exactly” the same number (N_{MAX}) of bubbles

Since the host knows the “secret” (i.e., the design of the warhead), she can individually preload pairs of detectors for every orientation/direction so that they will be “topped up” to N_{MAX} during the measurement

Before measurement



After measurement

Preload is unknown to inspector, i.e., bubble detectors are “wrapped in black tape”

For every position, inspector chooses, which detector (A_i, B_i) to use on golden warhead or on test item

(so that it becomes impossible for the host to conceal a spoof by unequally initializing the detectors)

Inspection Protocol

(simplified)

Template
(“Golden warhead”)
selected at deployment site

1

Warheads offered for inspection/dismantlement
(presumably already in storage)

Template and test items are placed in sealed containers

2

All items are brought to a dedicated dismantlement facility

Inspector announces which detector positions she wants to measure

3

Host prepares suite of bubble detectors

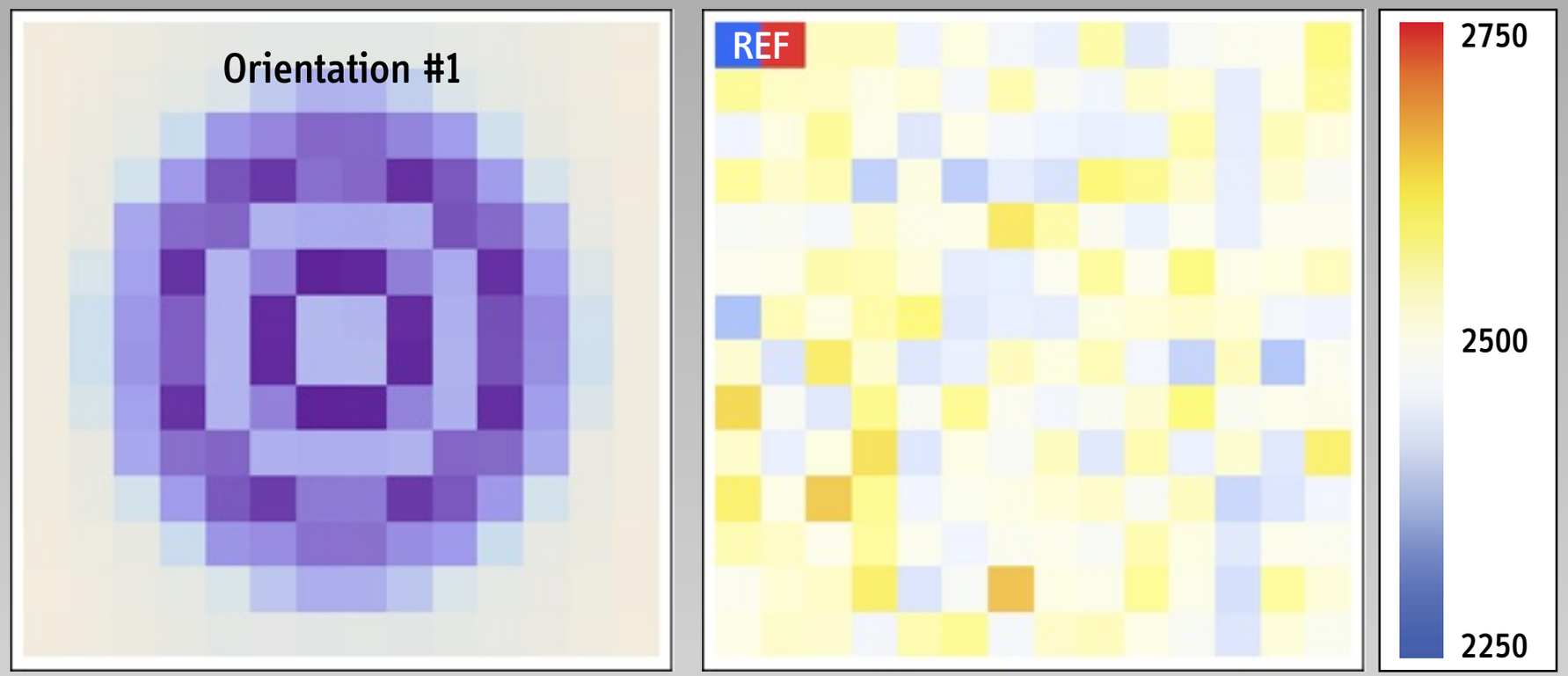
Inspection is carried out (template vs test item)

4

Inspector finds the number N_{max} in all measurements

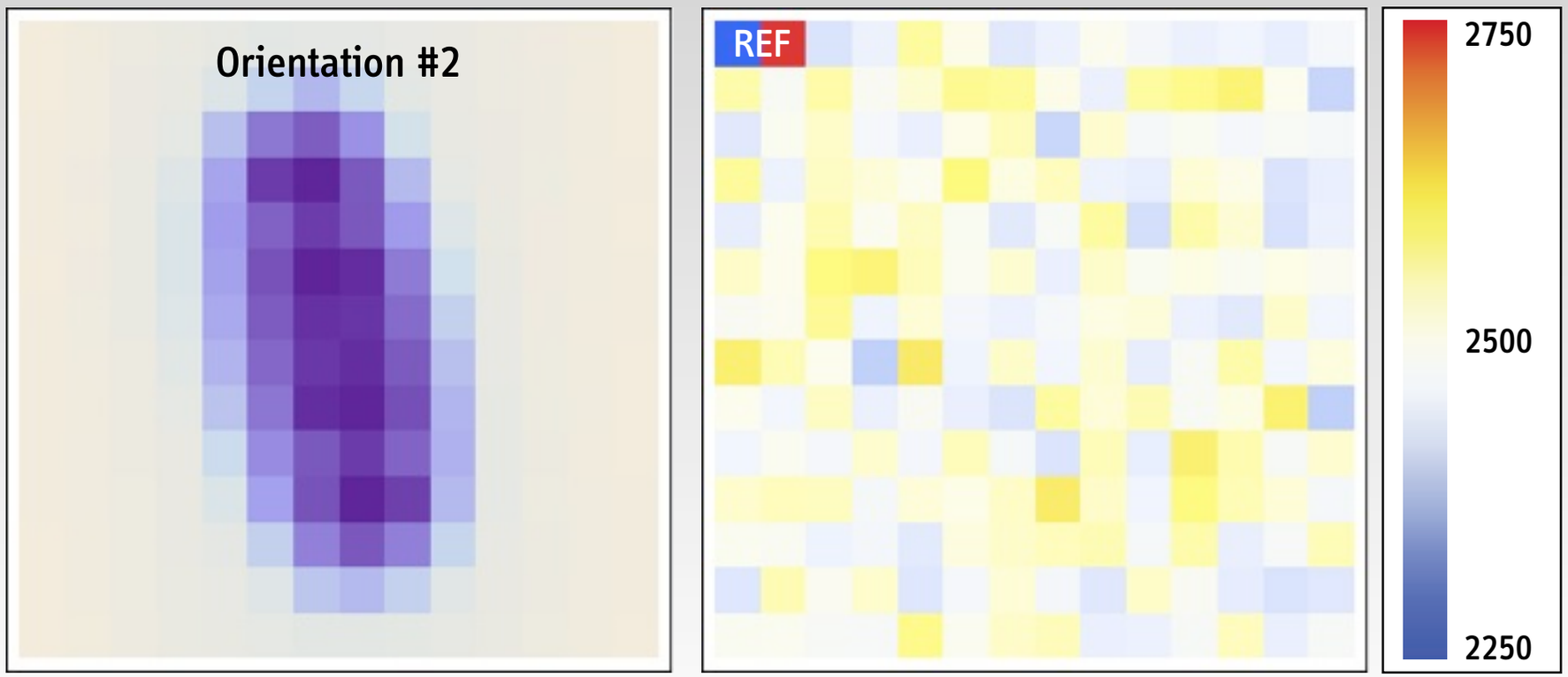
Does It Work?

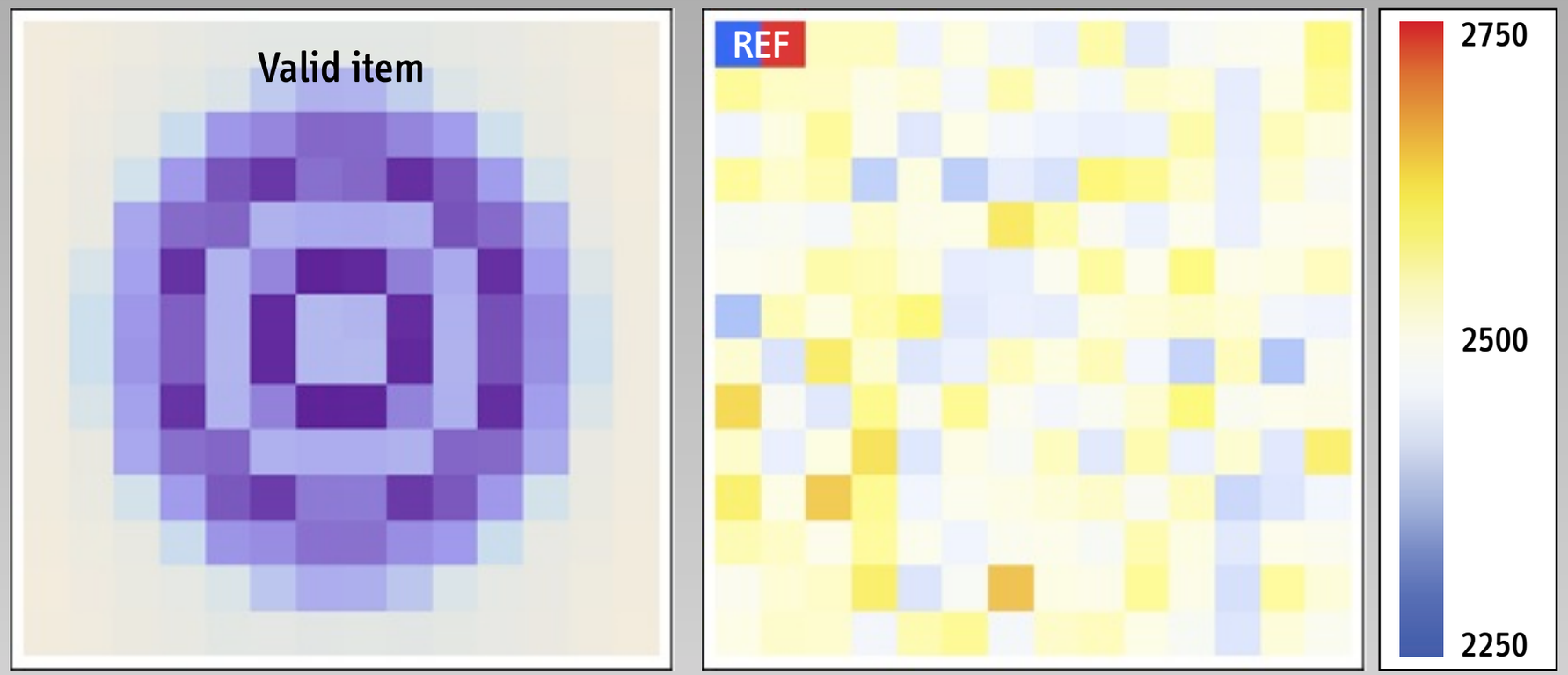
Results of Monte Carlo Neutron Transport Simulations



Radiograph (never measured)

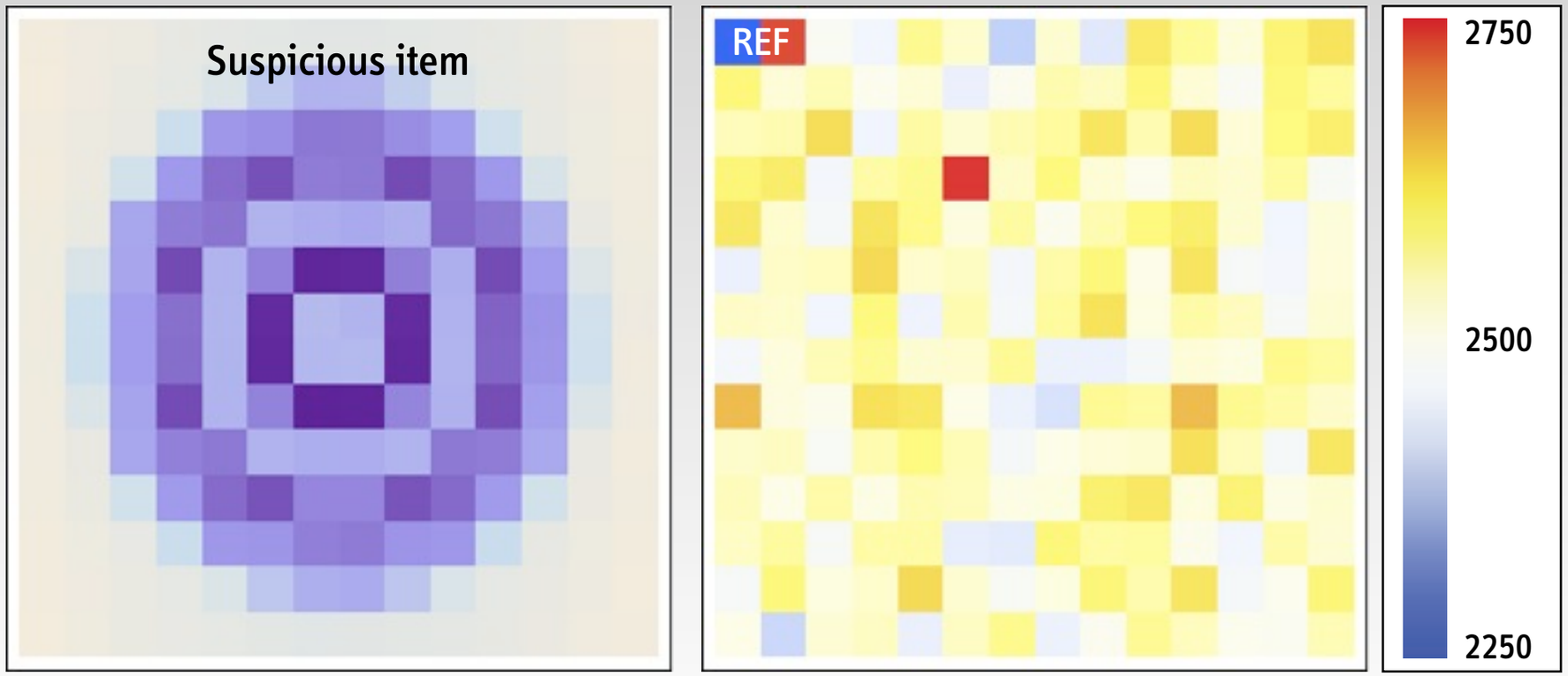
Bubble count after inspection





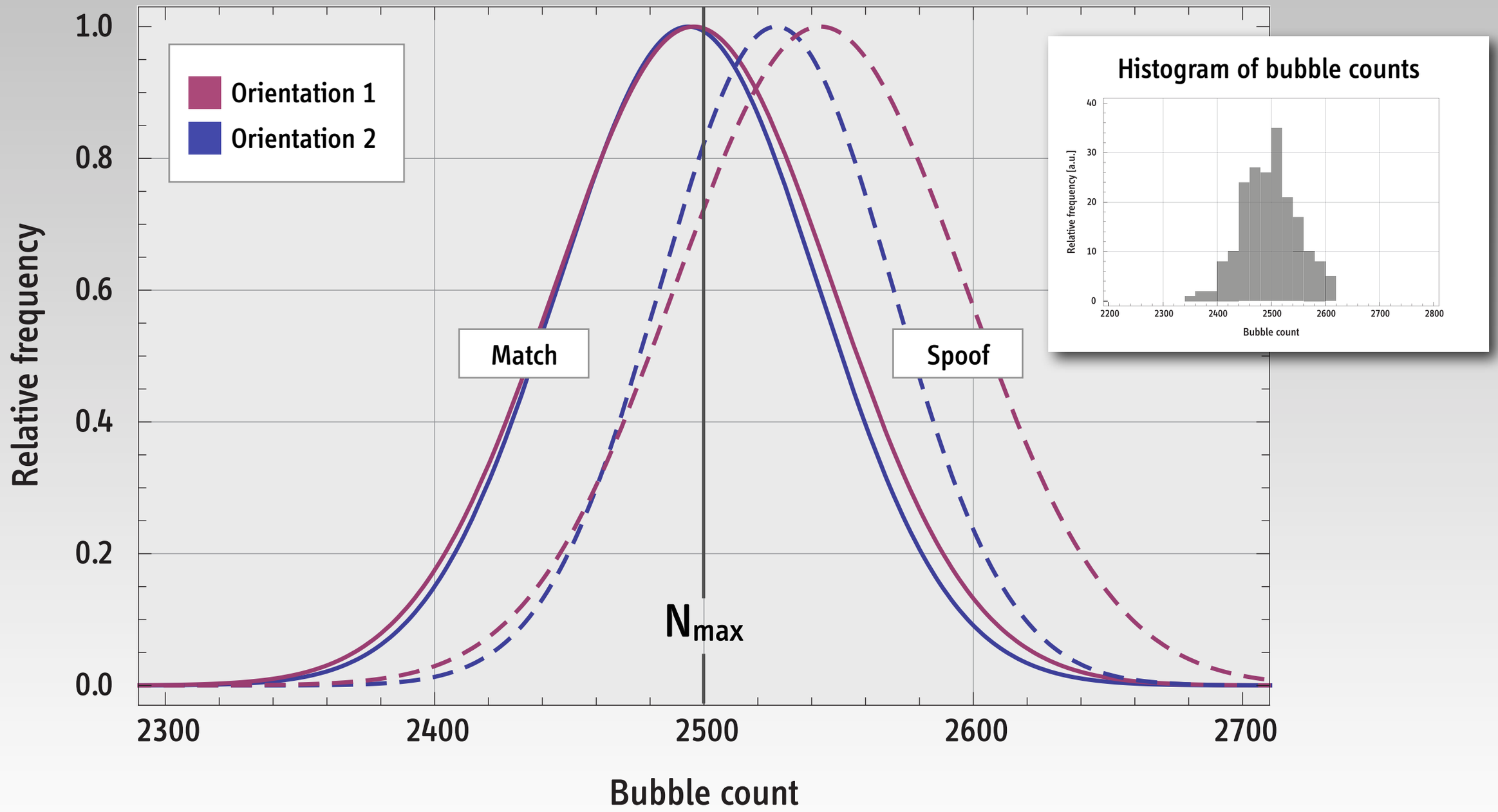
Radiograph (never measured)

Bubble count after inspection



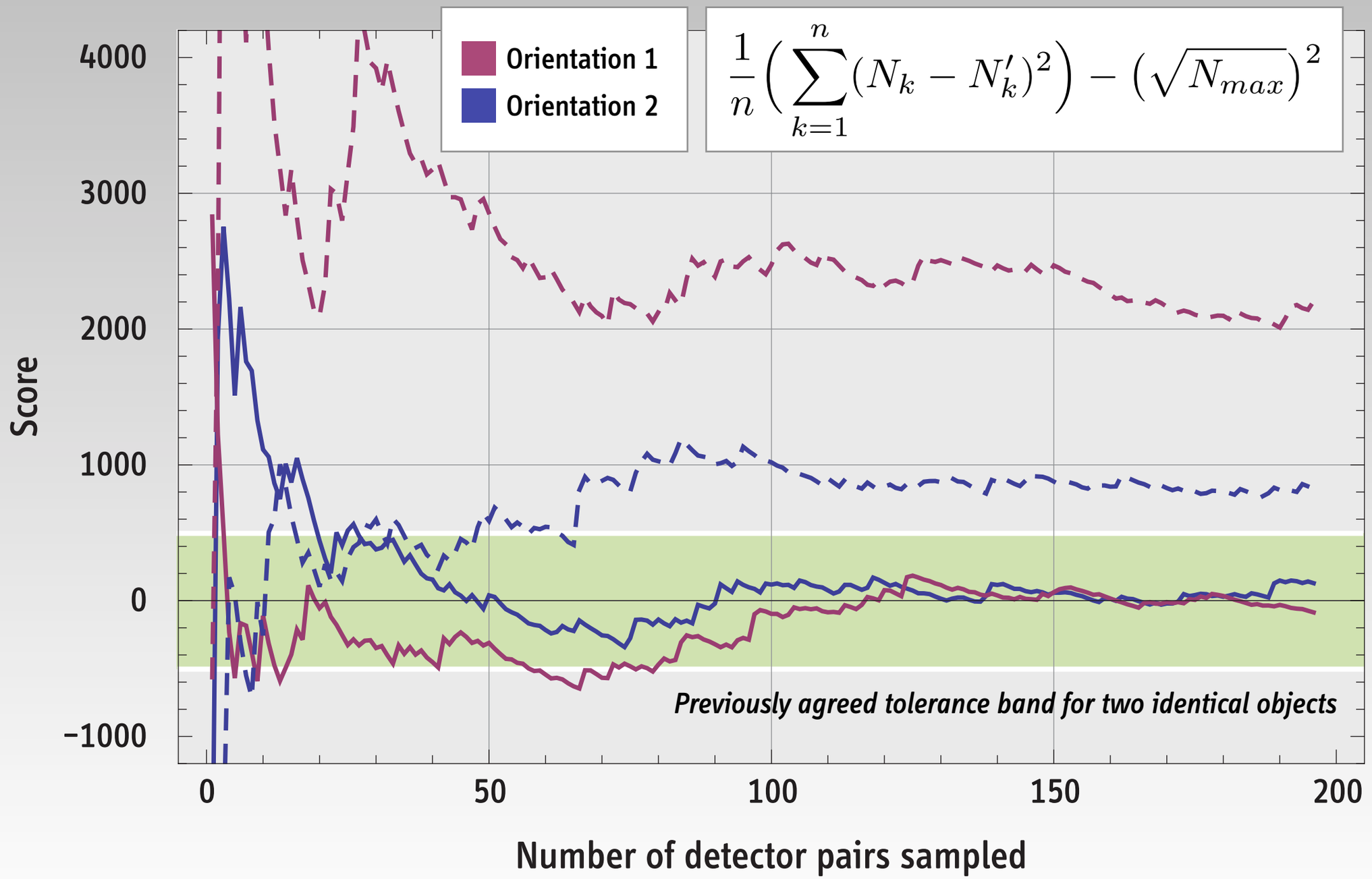
Bubble-count Distributions from Valid Items and Spoofs Can Be Distinguished

(Sample fits to data from 14 x 14 = 196 bubble detectors in previous example)



How Many Detector Pairs Have to be Sampled?

Depending on the orientation of the test item, 50–100 samples might be sufficient



Way Forward

Provide proof-of-concept experimentally

Zero-knowledge protocols appear as an important new approach to nuclear warhead verification

Concepts and technologies need to be developed now in order to be available for the next round of arms-control negotiations