A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol

Alexander Glaser

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

Princeton Plasma Physics Laboratory
May 16, 2012

Revision 8

A New Era of Nuclear Disarmament?

“We endorse setting the goal of a world free of nuclear weapons and working energetically on the actions required to achieve that goal.”

A World Free of Nuclear Weapons
George P. Shultz, William J. Perry, Henry A. Kissinger, and Sam Nunn
The Wall Street Journal, January 4, 2007

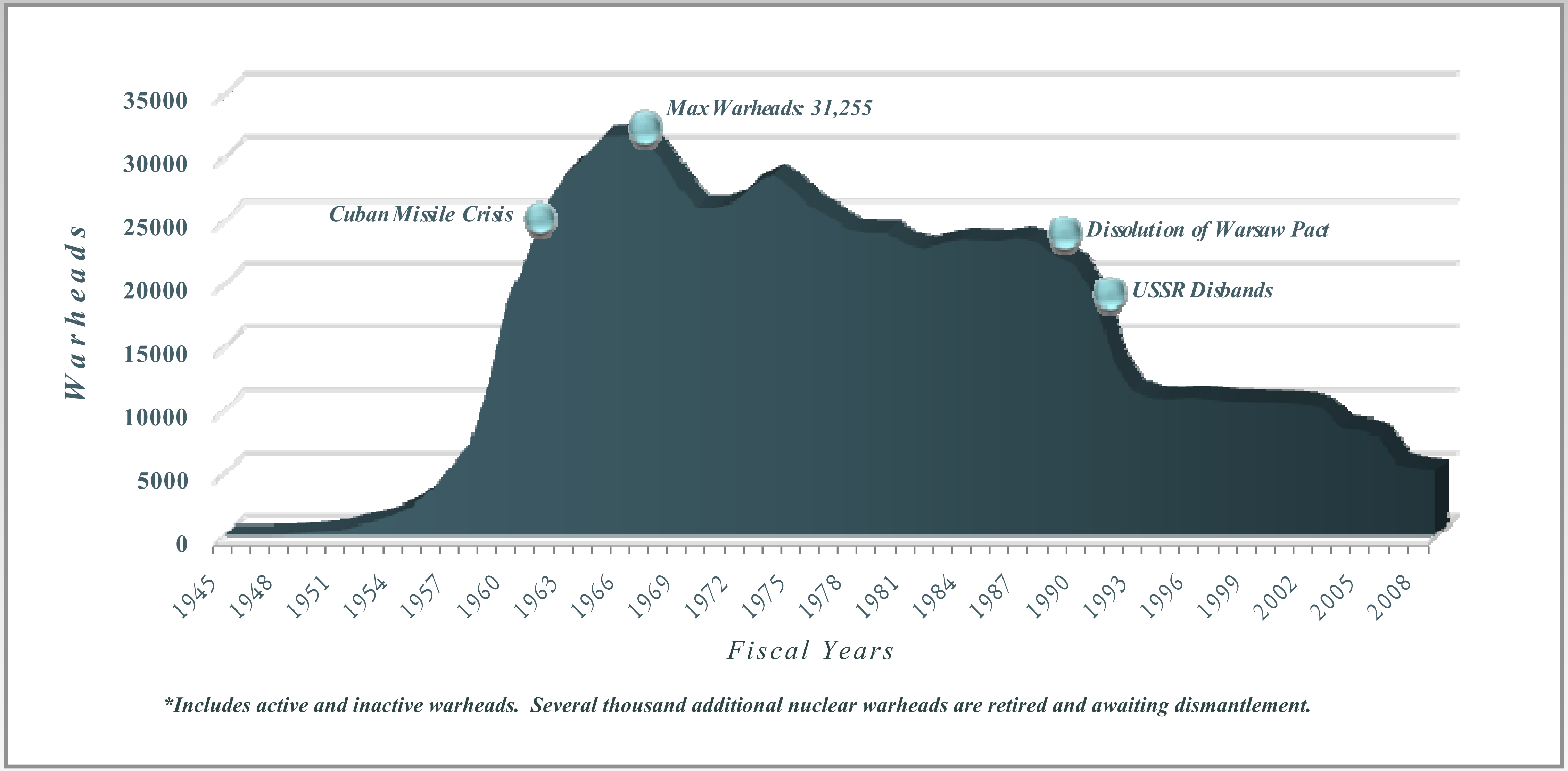
“While the new START treaty is an important step forward, it is just one step on a longer journey. As I said last year in Prague, this treaty will set the stage for further cuts. And going forward, we hope to pursue discussions with Russia on reducing both our strategic and tactical weapons, including non-deployed weapons.”

U.S. President Obama, upon signing the New START Treaty, April 2010

U.S. Nuclear Weapons Stockpile, 1945–2009

5,113 warheads in stockpile, as of September 2009

(1,665 operationally deployed strategic warheads, as of September 2011)



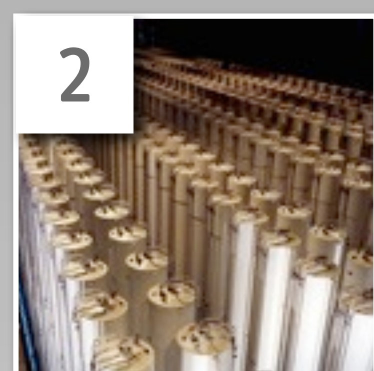
Increasing Transparency in the U.S. Nuclear Weapons Stockpile, Fact Sheet, U.S. Department of Defense, Washington, DC, 3 May 2010

Making and Dismantling Nuclear Weapons

Making Nuclear Weapons

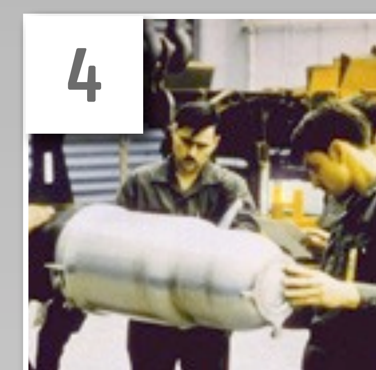
Source material (Uranium)

Uranium enrichment

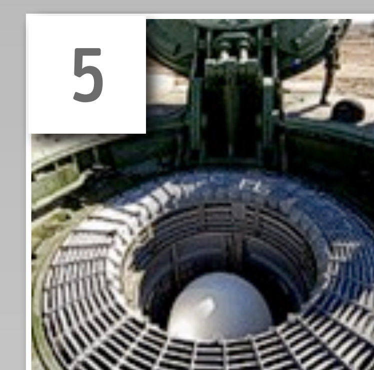


Plutonium production

Production of weapon components

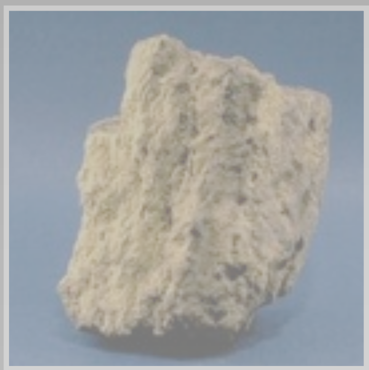


Warhead / Weapon assembly



Deployment

Dismantling Nuclear Weapons

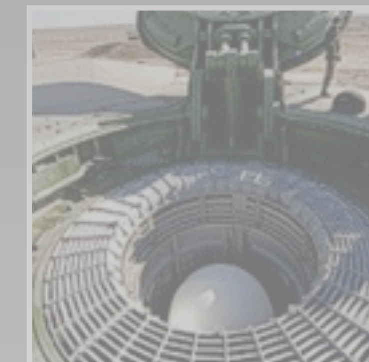


Source material (Uranium)

Plutonium production or uranium enrichment

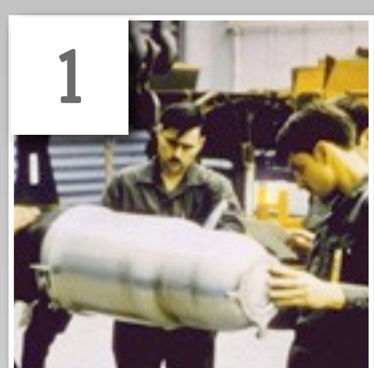
Production of weapon components

Warhead / Weapon assembly



Deployment

1

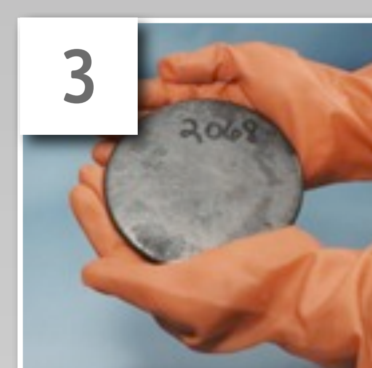


Warhead / Weapon disassembly

2

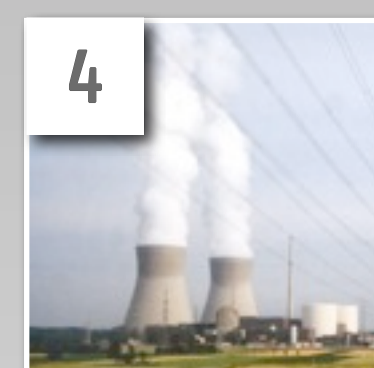
Recovery of weapon components

3



Recovery of fissile material

4



Elimination/disposition of fissile material

Key Stages for a Verification Approach

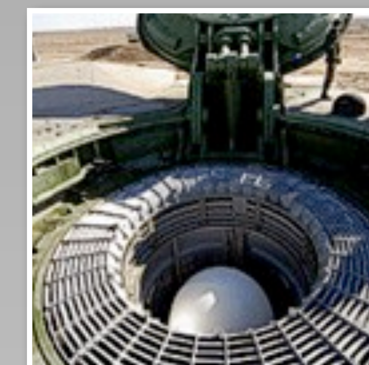
(going beyond verifying limits on deployed nuclear weapons)

Source material
(Uranium)

Plutonium production or
uranium enrichment

Production of
weapon components

Warhead / Weapon
assembly



Deployment

Warhead / Weapon
disassembly

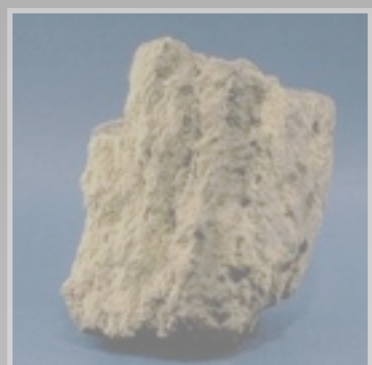
Recovery of
weapon components

Recovery of
fissile material

Elimination/disposition
of fissile material

Key Stages for a Verification Approach

(going beyond verifying limits on deployed nuclear weapons)

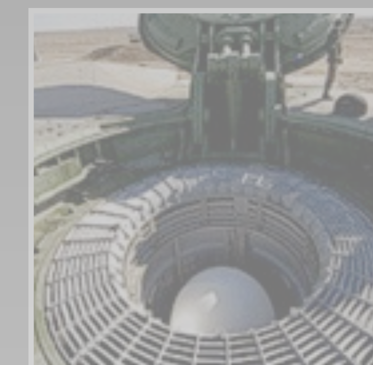


Source material (Uranium)

Plutonium production or uranium enrichment

Production of weapon components

Warhead / Weapon assembly



Deployment

Warhead / Weapon disassembly

Recovery of weapon components

Recovery of fissile material

Elimination/disposition of fissile material

Components of a U.S. B-61 Thermonuclear Weapon

Source: U.S. Department of Energy

How Can the Inspecting Party Be Assured That a Genuine Warhead is Being Presented?

<u>Hypothetical scenarios that a country "hedging its bets" might consider</u>

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 containing some fissile material)
Objective: Withhold real warheads

Present complete but obsolete warheads that may (or may not) contain less fissile material
Objective: Withhold fissile material or specific (more advanced) warheads

Requirements for an Inspection System

Certification

Assuring the host that the system does not divulge information that would be considered proliferation-sensitive or be otherwise classified

Authentication

Assuring the inspecting party that the instrument works as designed and that the data collected and displayed during the inspection are genuine measurements

Completeness and Soundness of Approach

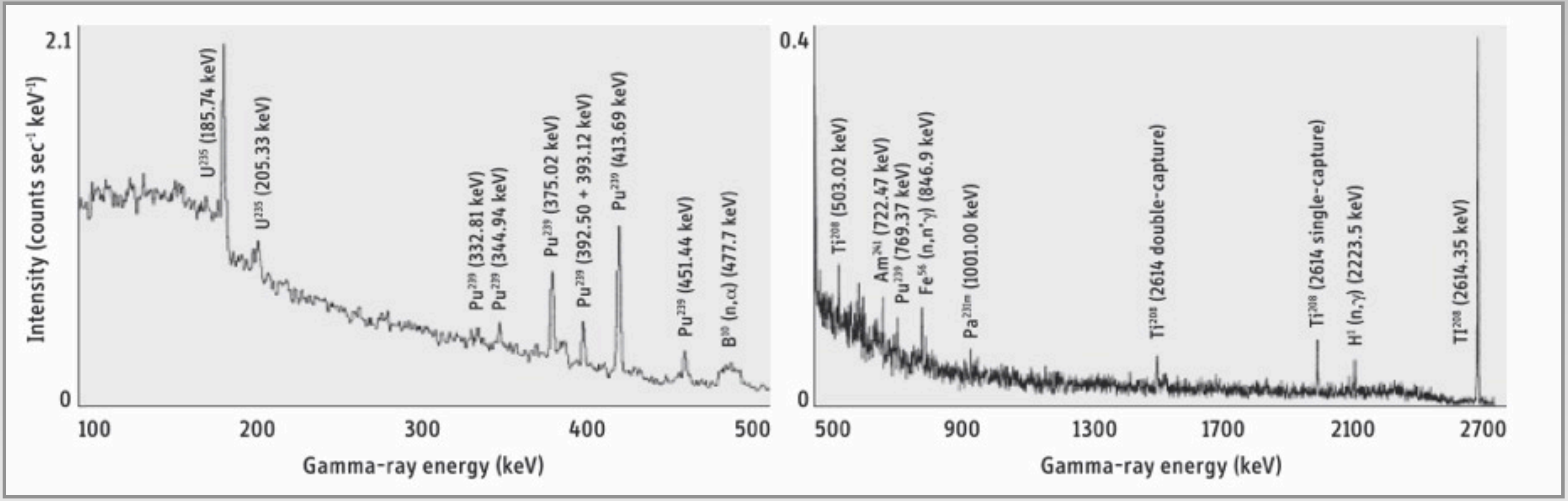
If a valid item is presented, then the item is accepted with high probability

If an invalid item is presented, then the item is rejected with high probability
(in spite of elaborate deception efforts that the host might undertake)

Previous Verification Efforts

Nuclear Warheads Have Unique Signatures

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

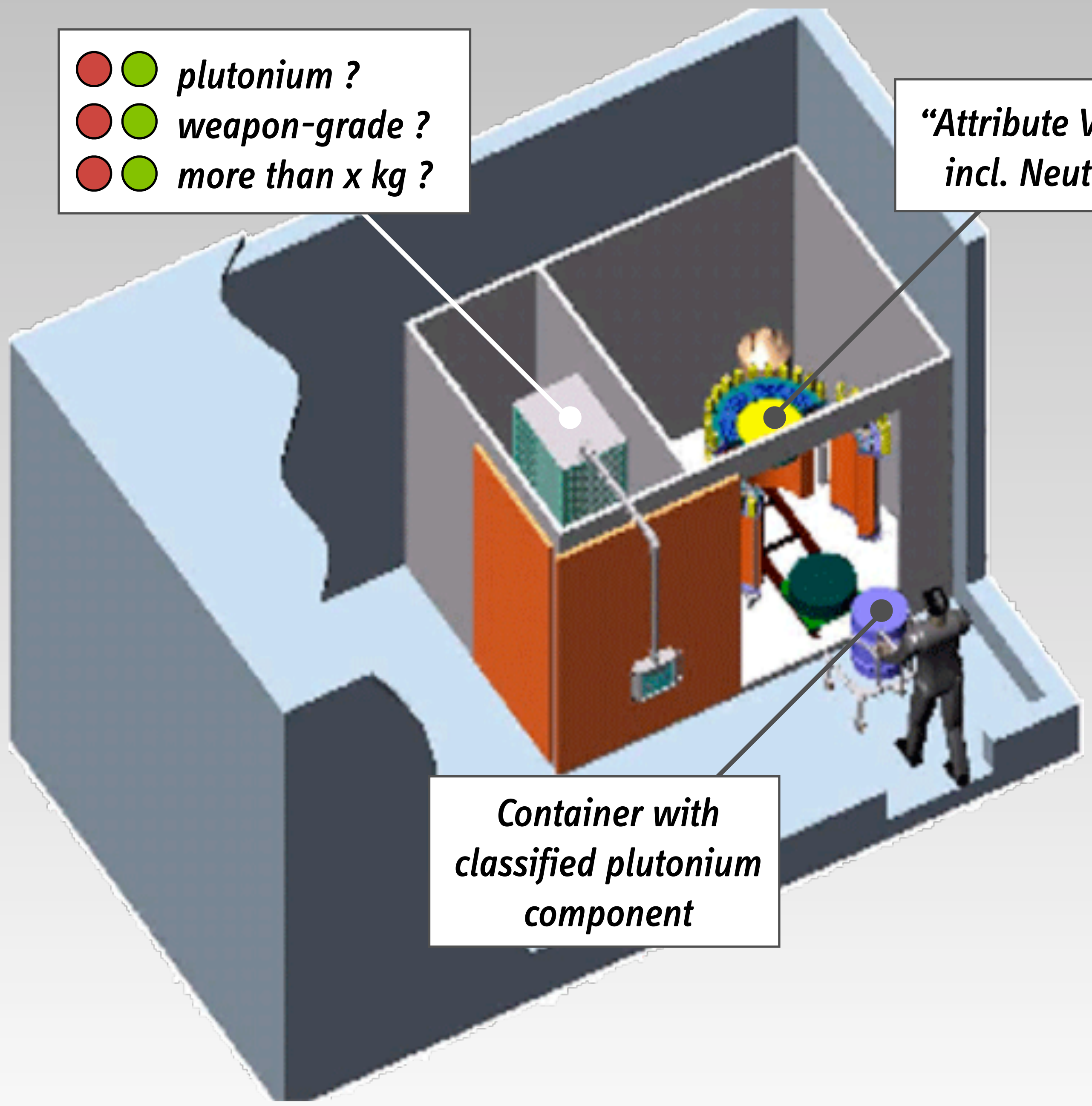


Gamma radiation spectrum from a Soviet warhead measured in 1989

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

"Attribute Approach"

Confirming Selected Characteristics of an Object in Classified Form



1996–2002 Trilateral Initiative developed approach to determine that a container holds more than a threshold amount of weapon-grade plutonium.

Results communicated by red or green lights through information barrier

BUT: Attributes are not defining enough for warhead differentiation and are likely to be at a significant risk of spoofing

"Template Approach"

Verifying that a warhead offered for inspection
is substantially identical to a reference warhead of the same type
that has been previously confirmed to be authentic

Measurements designed to generate "unique fingerprints" of the interrogated objects

Types of measurements are *a priori* unspecified
(typically neutron or gamma-spectroscopy)

Standard assumption: use of information barriers is critical and inevitable

Use of information barriers is generally problematic
(because sensitive data is still detected/recorded and could be transmitted through backdoor)

Instruments proposed so far are complex and their certification/authentication difficult

Princeton MAE/PPPL Verification Project

Princeton MAE/PPPL 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 test item in which nuclear materials are replaced with "benign" alternatives
- Avoid or minimize role/use of information barriers
- Validate conceptual approach with MCNP simulations

Project currently funded by Global Zero (www.globalzero.org)
and supported by PPPL Proposal Development Funds

What We Don’t Use

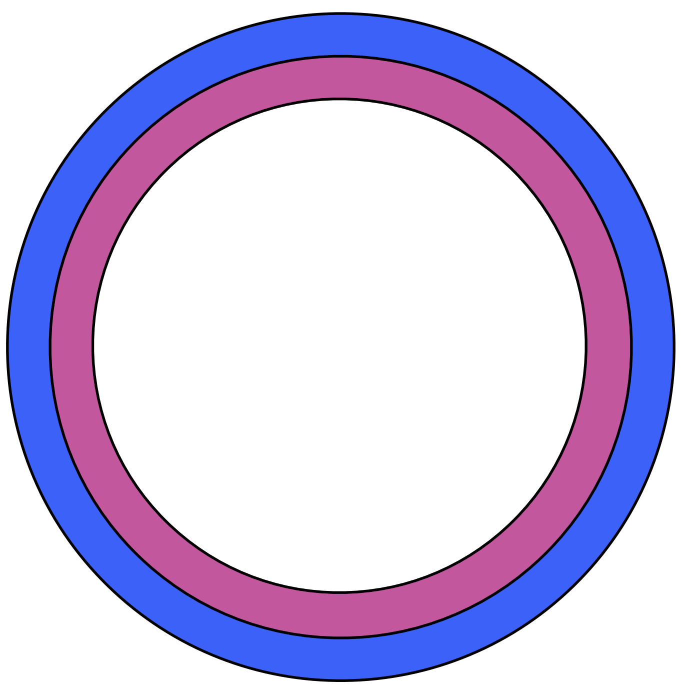
(and Don’t Need for Our Proof-of-concept)

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

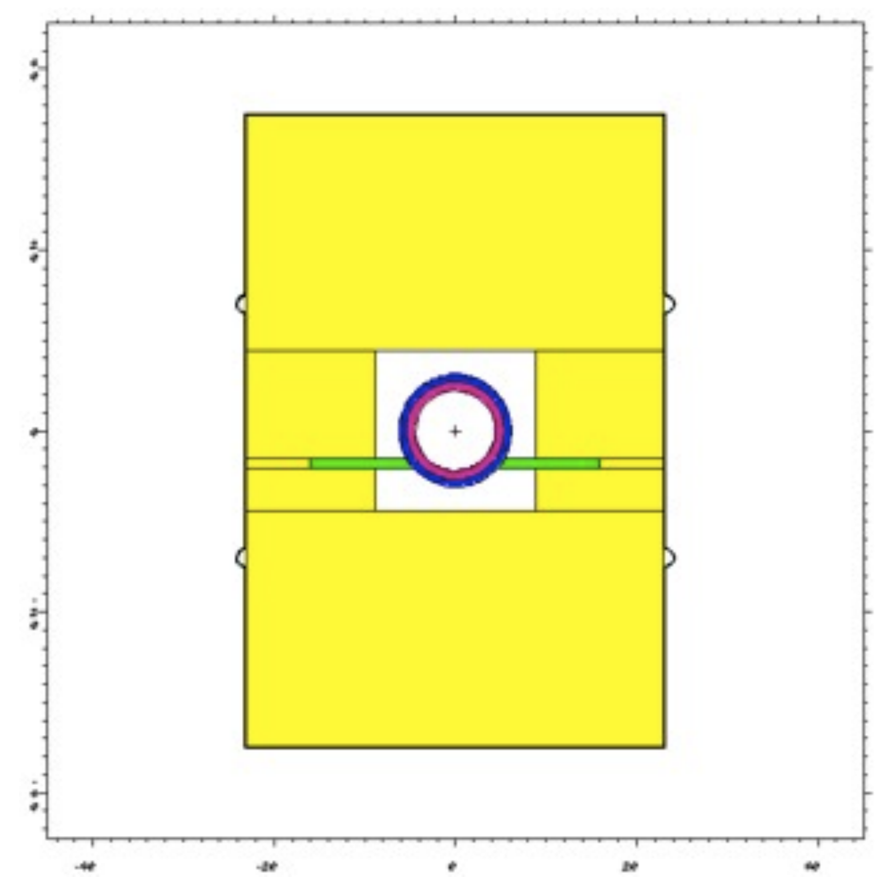
(Note: the final W62 was dismantled in August 2010, www.energy.gov/articles/dismantling-history-final-w62-warhead)

Simple Pit Configuration

("Test Item" in Standard Pit-Storage Container)

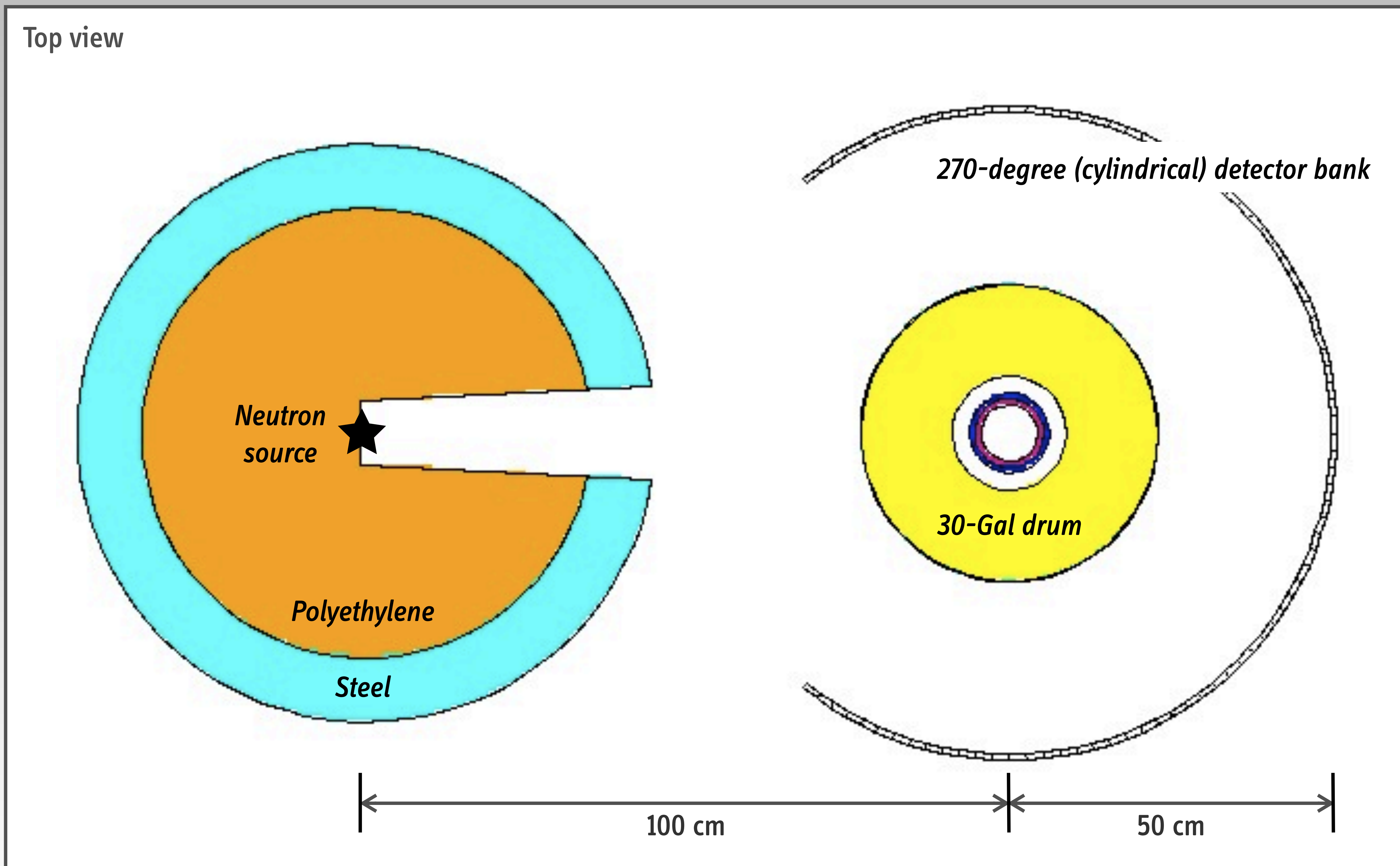


Plutonium/Lead shell, 4.75 kg, OD = 10.8 cm
Steel casing, OD = 12.4 cm



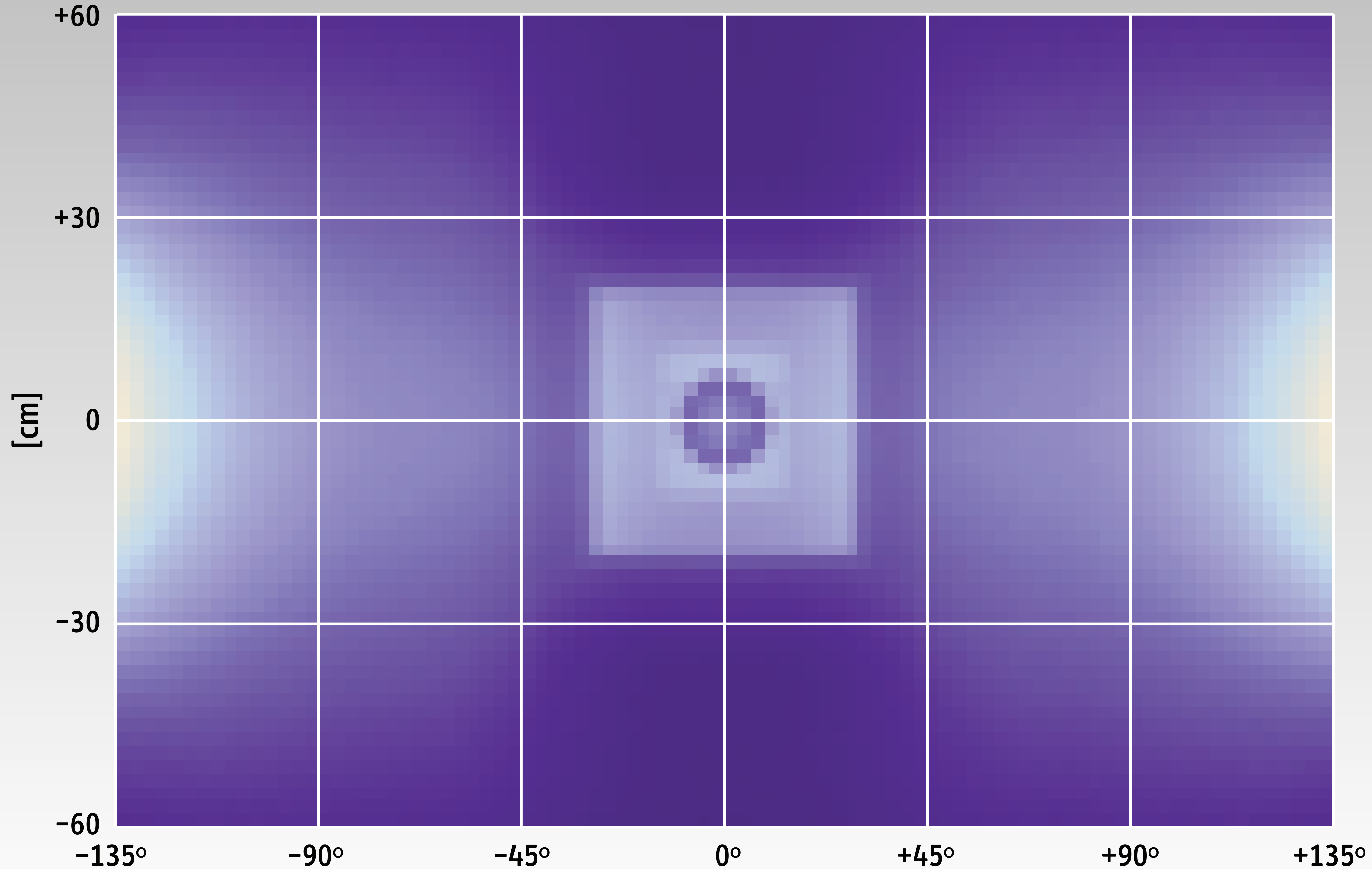
Celotex insulation and shock protection in standard 30-Gal steel drum

Neutron Source, Test Item, and Detector Bank



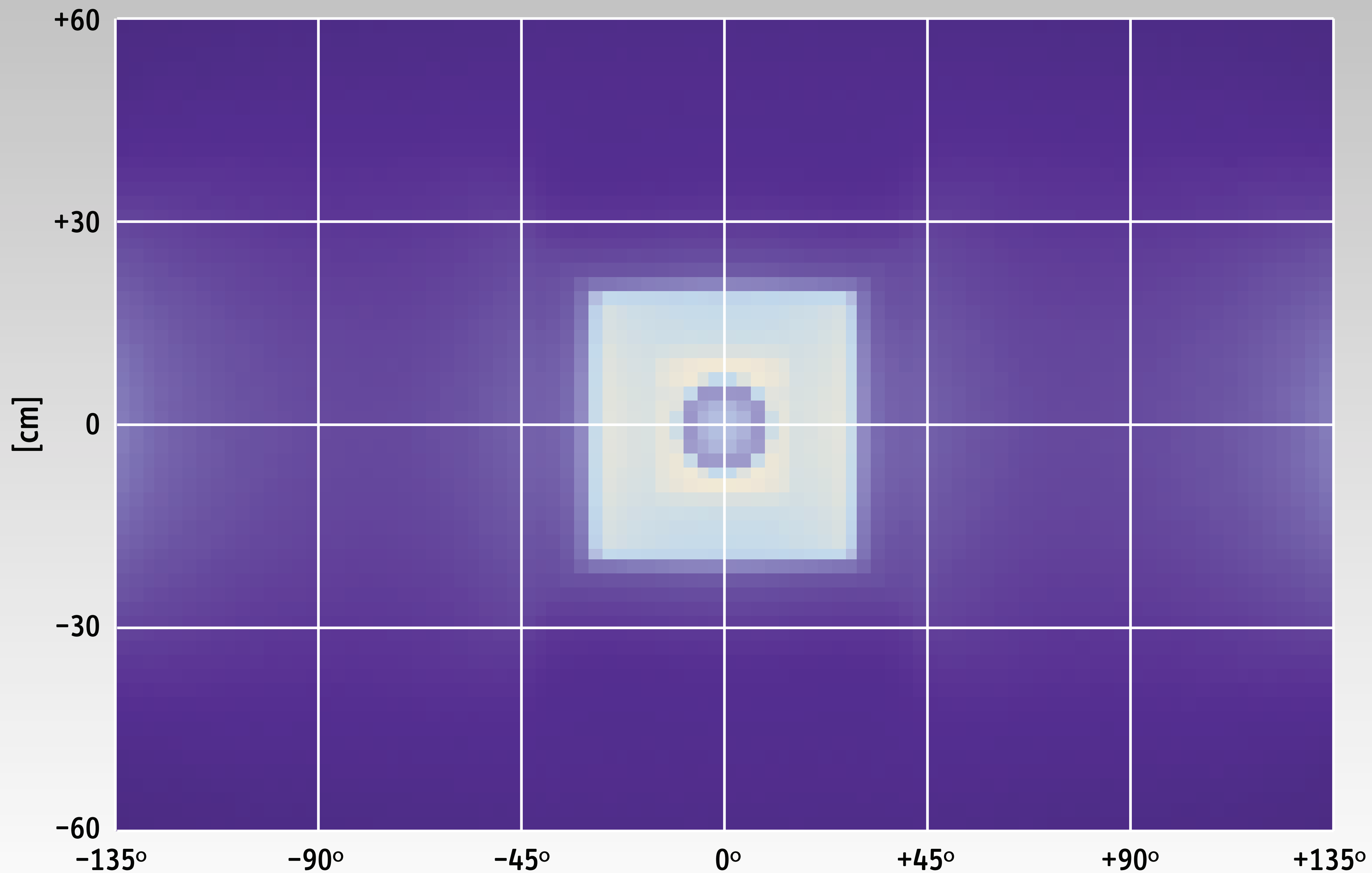
Radiograph of Test Item in Container

Simulated data, all neutron energies, MCNP5 simulations, 10 billion source neutrons



Radiograph of Test Item in Container

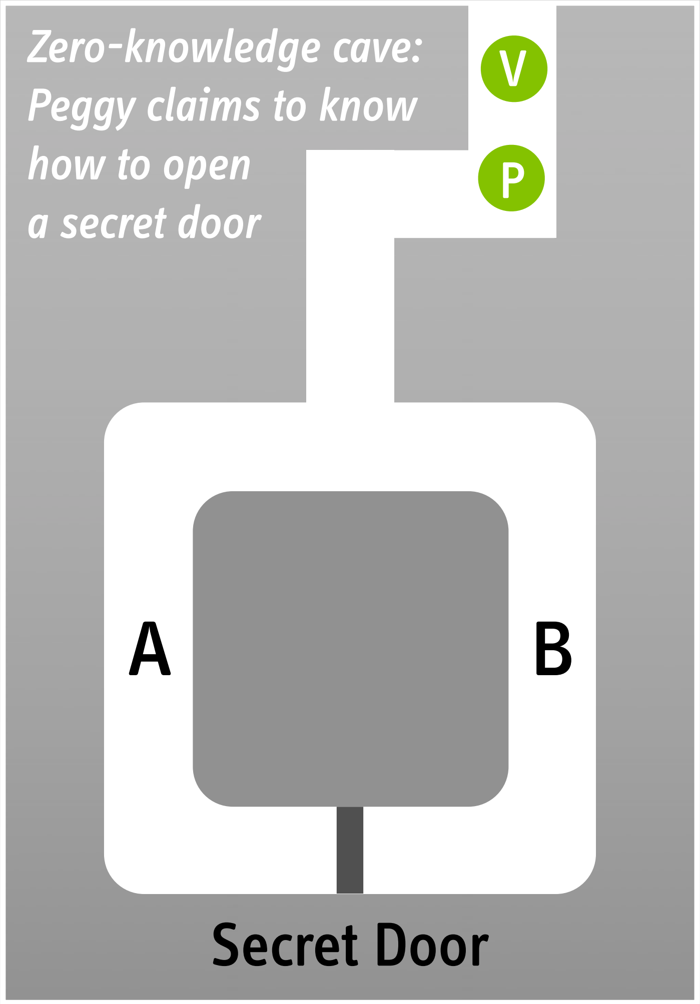
Simulated data, 14 MeV neutrons, MCNP5 simulations, 10 billion source neutrons

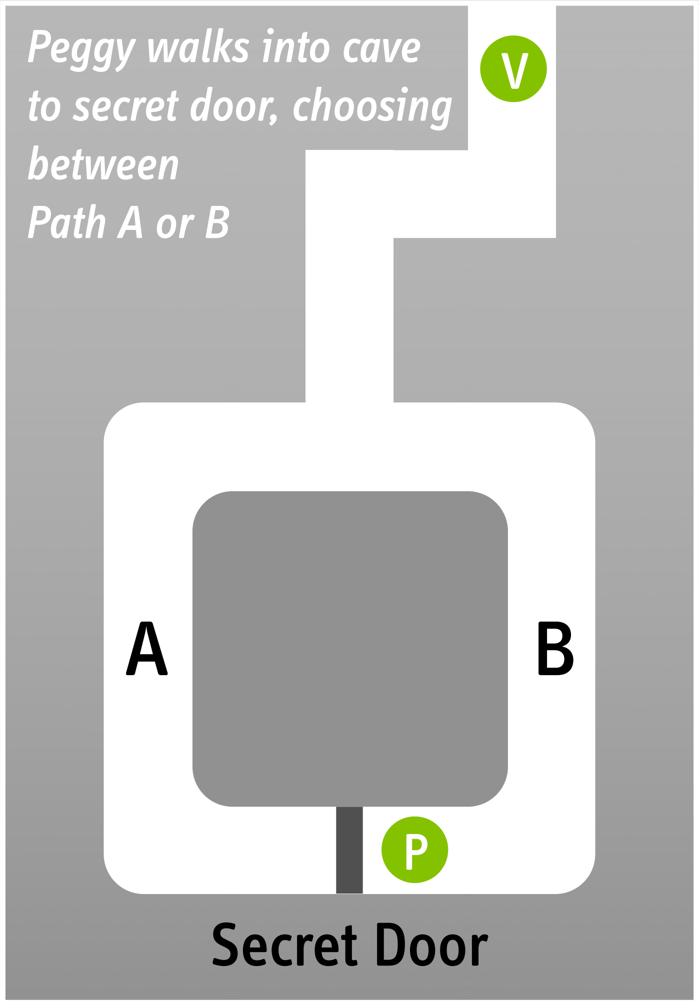


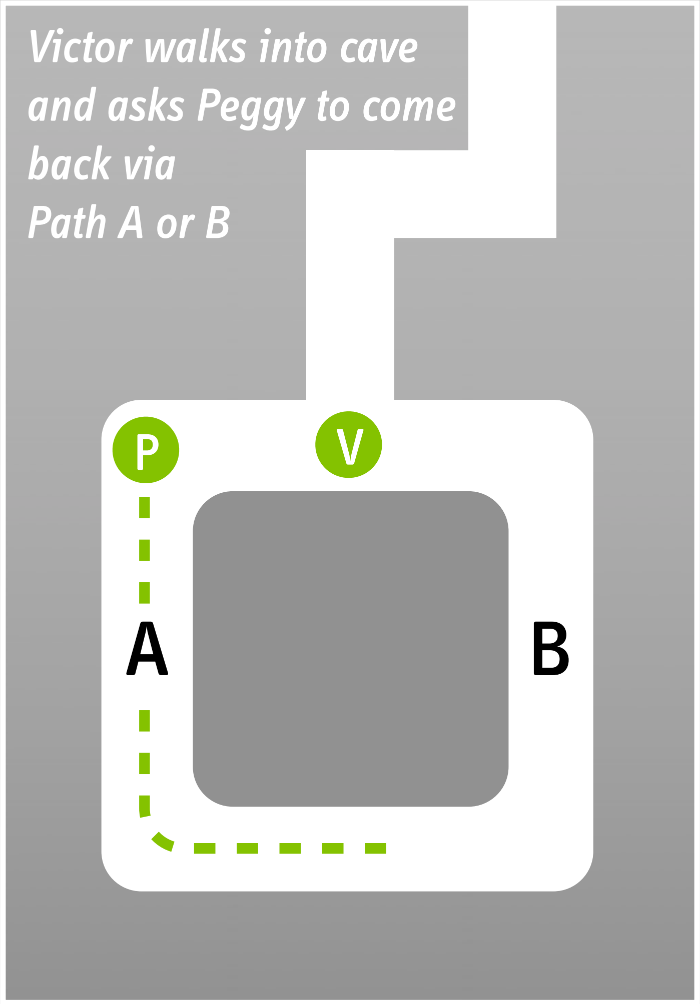
How Do We Prevent Sensitive Information from Being Detected?

Zero-Knowledge Protocols

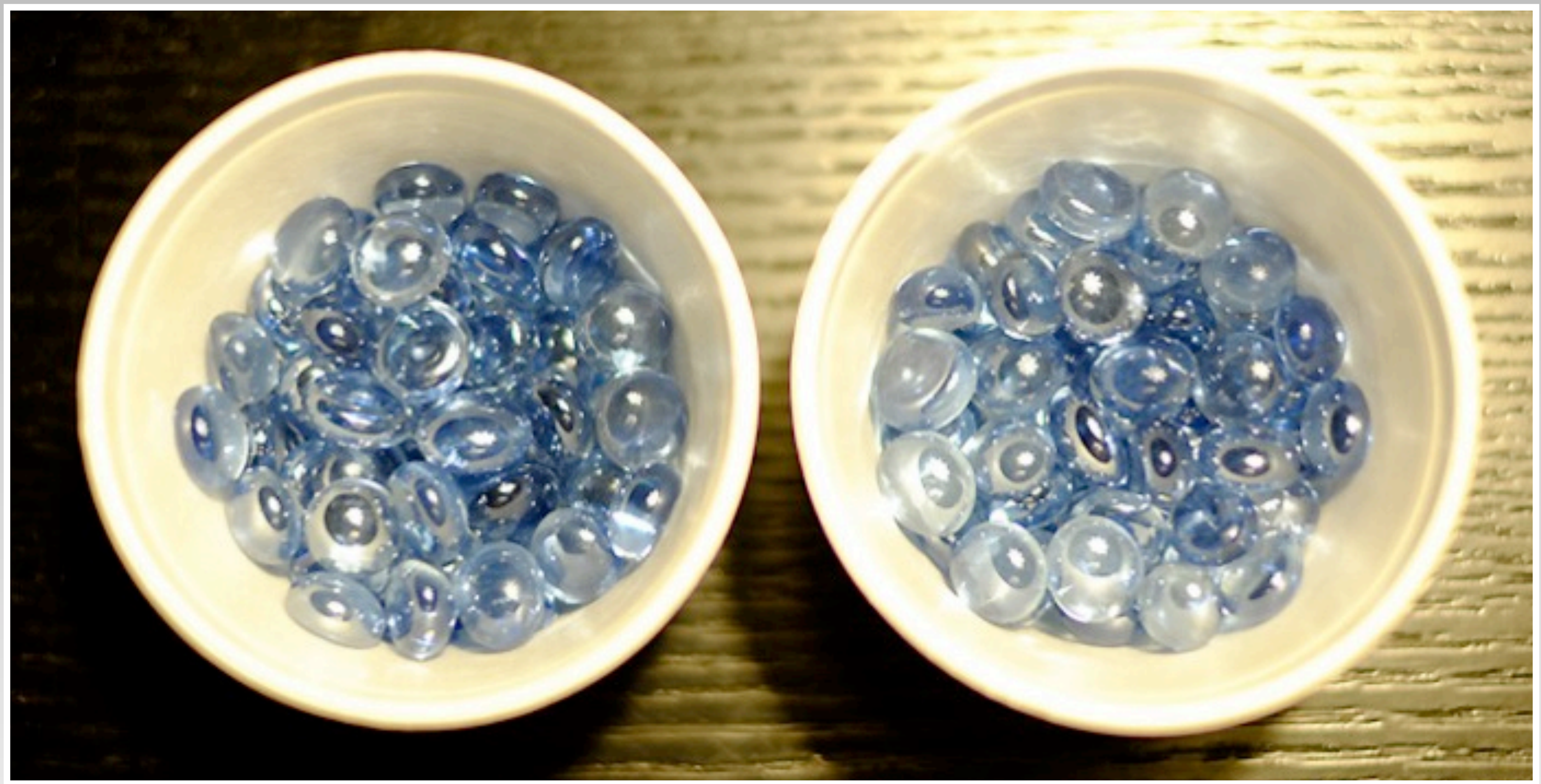
Zero-Knowledge Proofs: Peggy (P) proves to Victor (V) that she knows a secret without giving anything about the secret itself away







Another Example: “Marbles in a Cup”



Alice has two small cups each containing the same number of marbles. She wants to prove to Bob that both cups contain the same number of marbles without revealing to him what this number is.

Possible Hardware Implementations of a Zero-Knowledge Protocol for Warhead Verification

(TWO POTENTIAL OPTIONS)

Use neutron detector that does not (and cannot) display total count rates but only the remainder of a MOD[m,n] operation

n has to be small compared to the detector counts m
(otherwise design information would be preserved in the measurement)

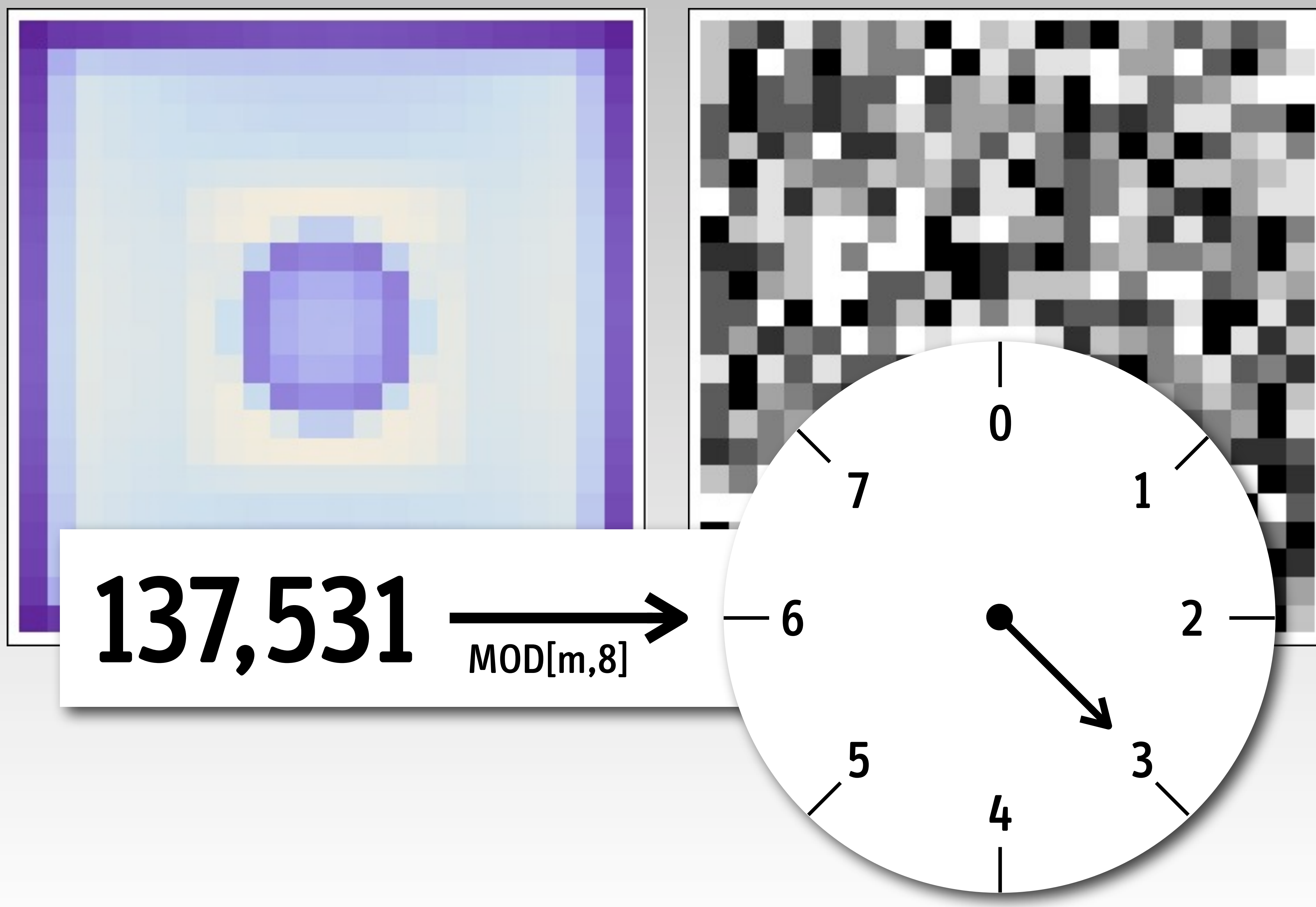
Use pair of (passive) detectors pre-initialized with random offset

(values unknown to inspecting party, but no incentive for host to cheat)
and compare absolute values only after measurements

MOD[m,n] Gate

Implementing a Simple MOD[m,n] Gate

"Dial of a Clock"



Implementing a Simple MOD[m,n] Gate

Selected Bits of a Binary Number

N = 137,531

N = 0 0 1 0 0 0 0 1 1 0 0 1 0 0 1 1 1 0 1 1

Design info / Drastic changes (0 0 1 0 0 0 0 1) — *Statistical noise ($\approx\sqrt{N}$)* (1 0 0 1 1 1 0 1 1)

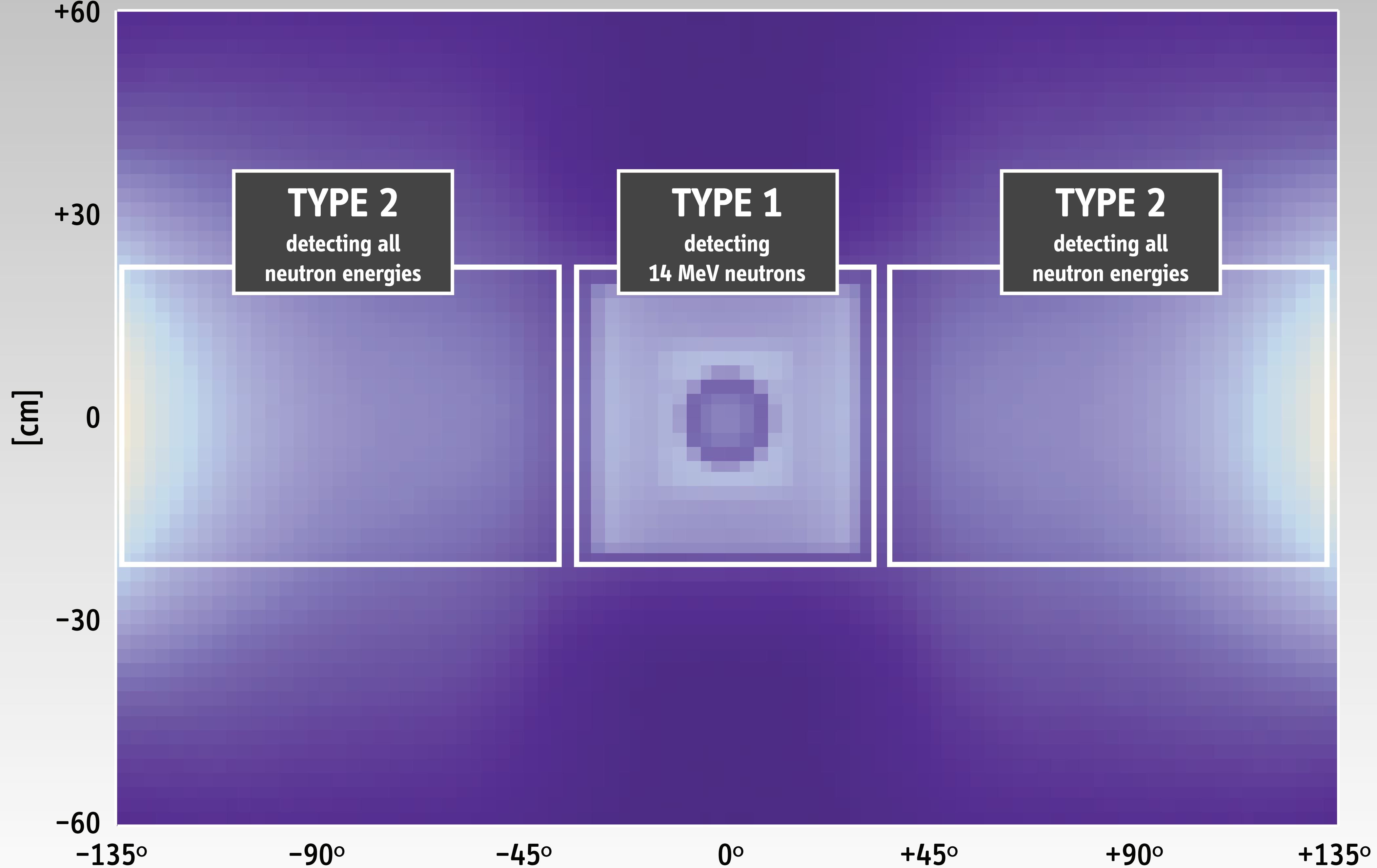
Select 1, 2, or 3 (middle) bits to detect only 2, 4, or 8 different values

Compare "distance" between measured values
(e.g. for MOD[m,8], distance between 0 and 7 is 1)

Results of Monte Carlo Neutron Transport Simulations

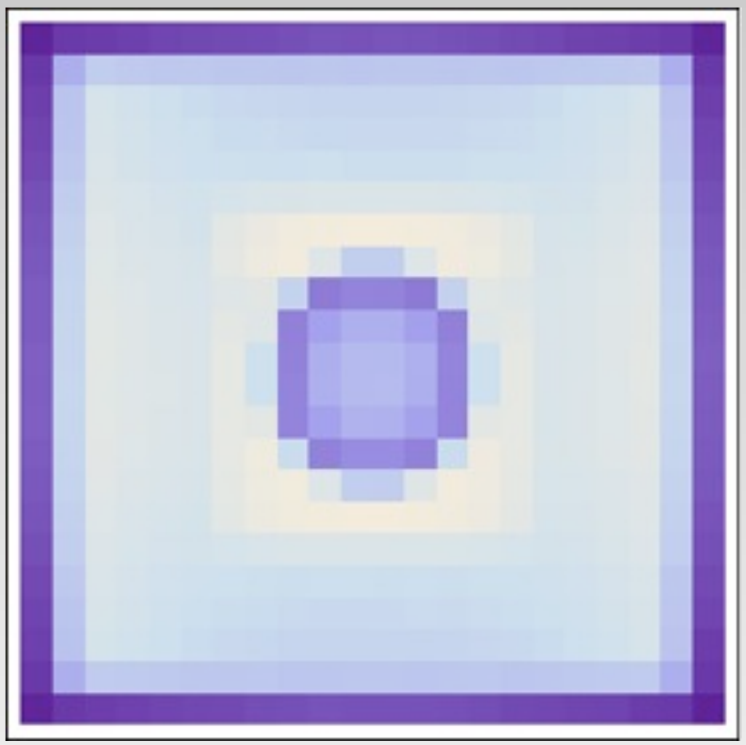
Radiograph of Test Item in Container

Consider detection of directly transmitted and scattered neutrons

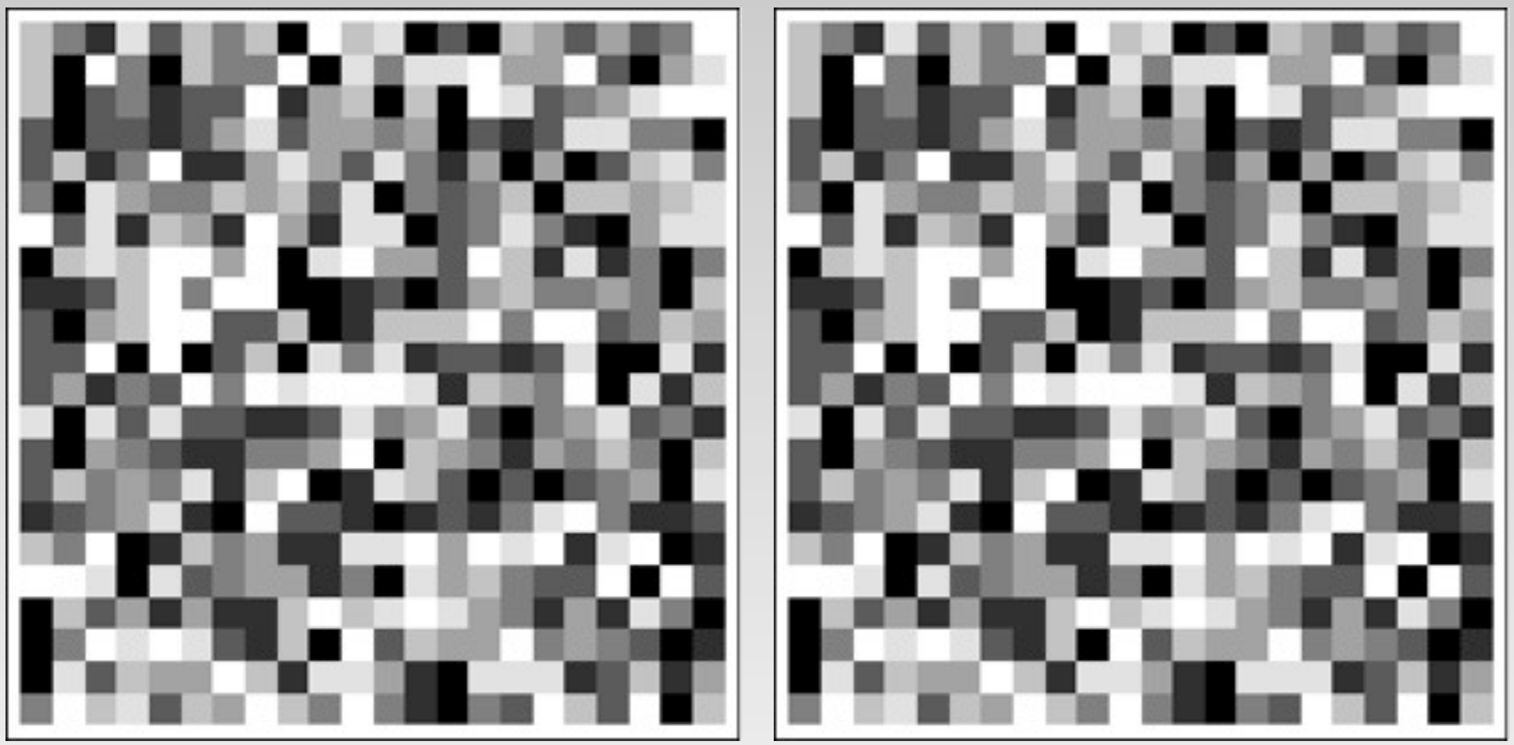


Before the measurements are carried out, a pair of detector arrays is initialized

Type 1 (transmission) measurement, 22x22 pixels

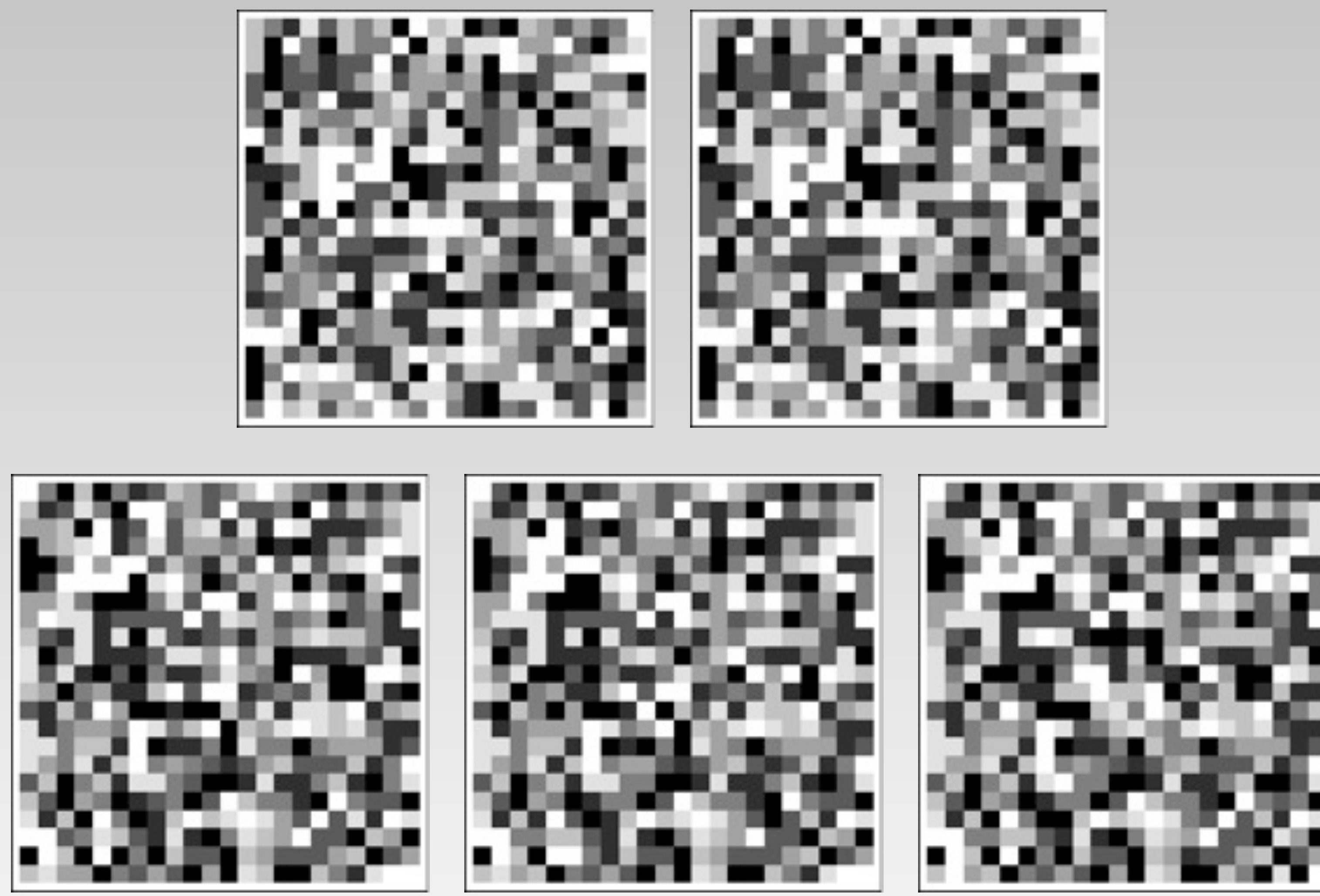


Radiograph
(never measured)



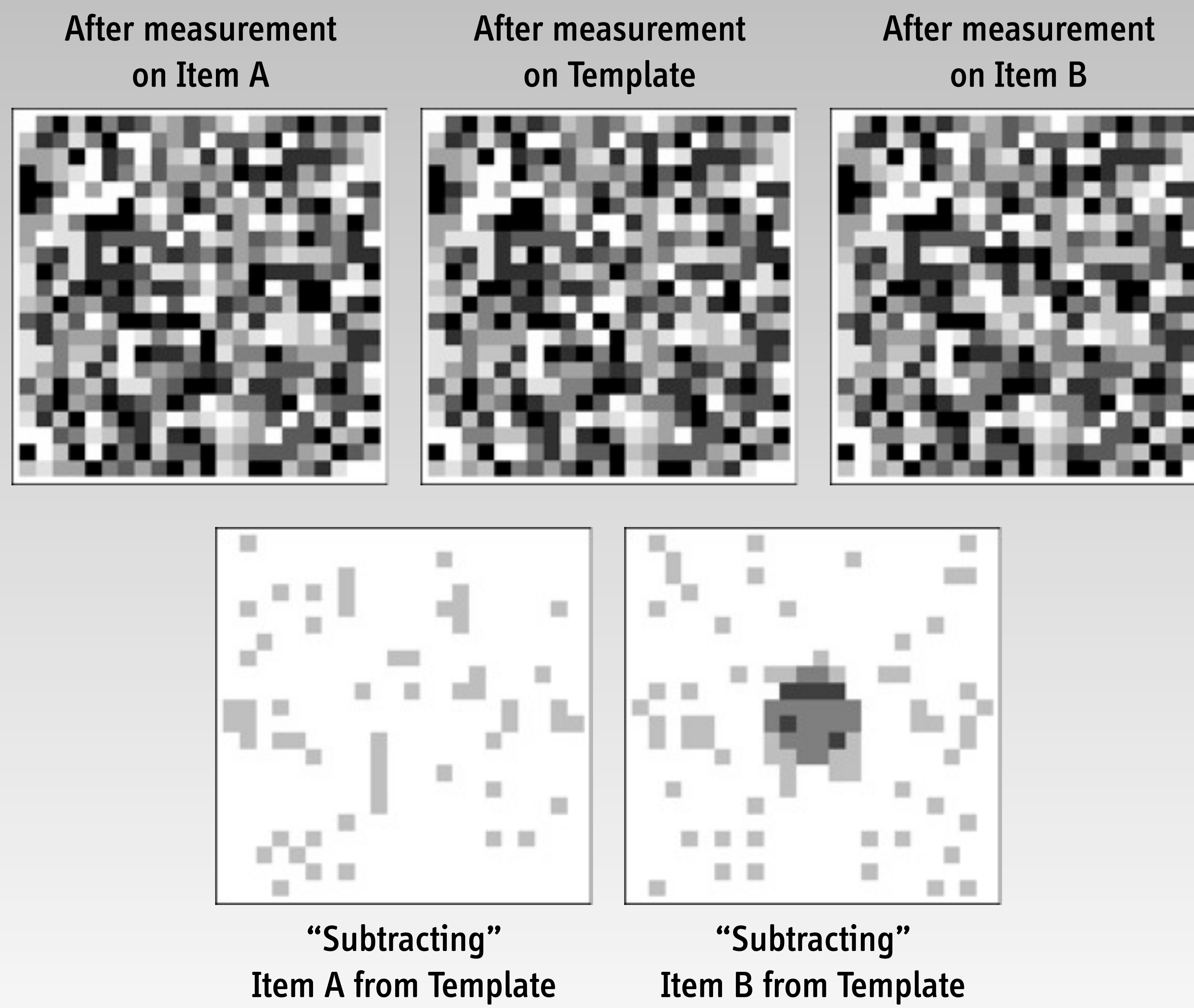
Pair of randomly but identically initialized
"MOD[m,n] detectors"
3 bits (8 possible values) per pixel

During the inspection, one detector array is used on the template, one on the test item



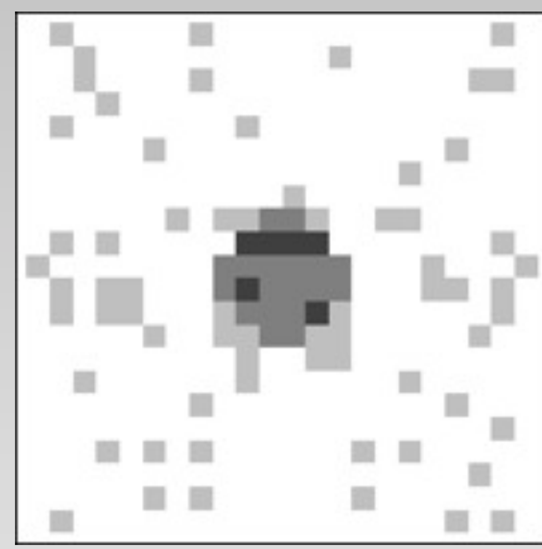
MCNP5 simulations, 10 billion source neutrons; average detector count: about 80,000 (17 bits), selected bits: 12, 13, 14

After the measurements, each detector array still features a random bit pattern, but …

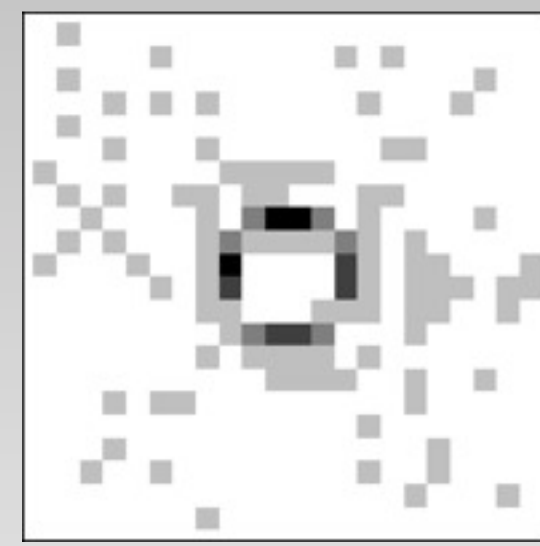


Many types of modifications can be detected in transmission measurements

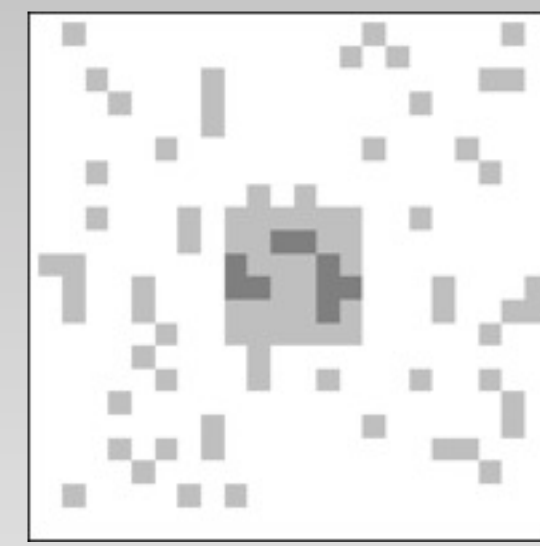
Match



800-gram diversion



Plutonium-dioxide
(same plutonium mass)



Lead

More sophisticated attacks may require (additional) measurements at large angles
where both scattered and fission neutrons are detected

Can It Be Built?

Passive Bubble Detectors

www.bubbletech.ca

Detectors with different neutron-energy thresholds are available
(no cutoff, 500 keV, 1 MeV, 10 MeV)

“Adding Marbles from a Cup to a Bucket”
Initialize detectors with random number of bubbles before measurement

Next Steps / Final Thoughts

Provide proof-of-concept experimentally

Determine the impact of "room return" and systematic errors
(e.g. detector drift between measurements)

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

(even if passive detector technologies prove difficult to use)

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

A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol

Alexander Glaser

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

Princeton Plasma Physics Laboratory
May 16, 2012