A ZERO-KNOWLEDGE PROTOCOL FOR NUCLEAR WARHEAD VERIFICATION

Alexander Glaser* and Robert J. Goldston**

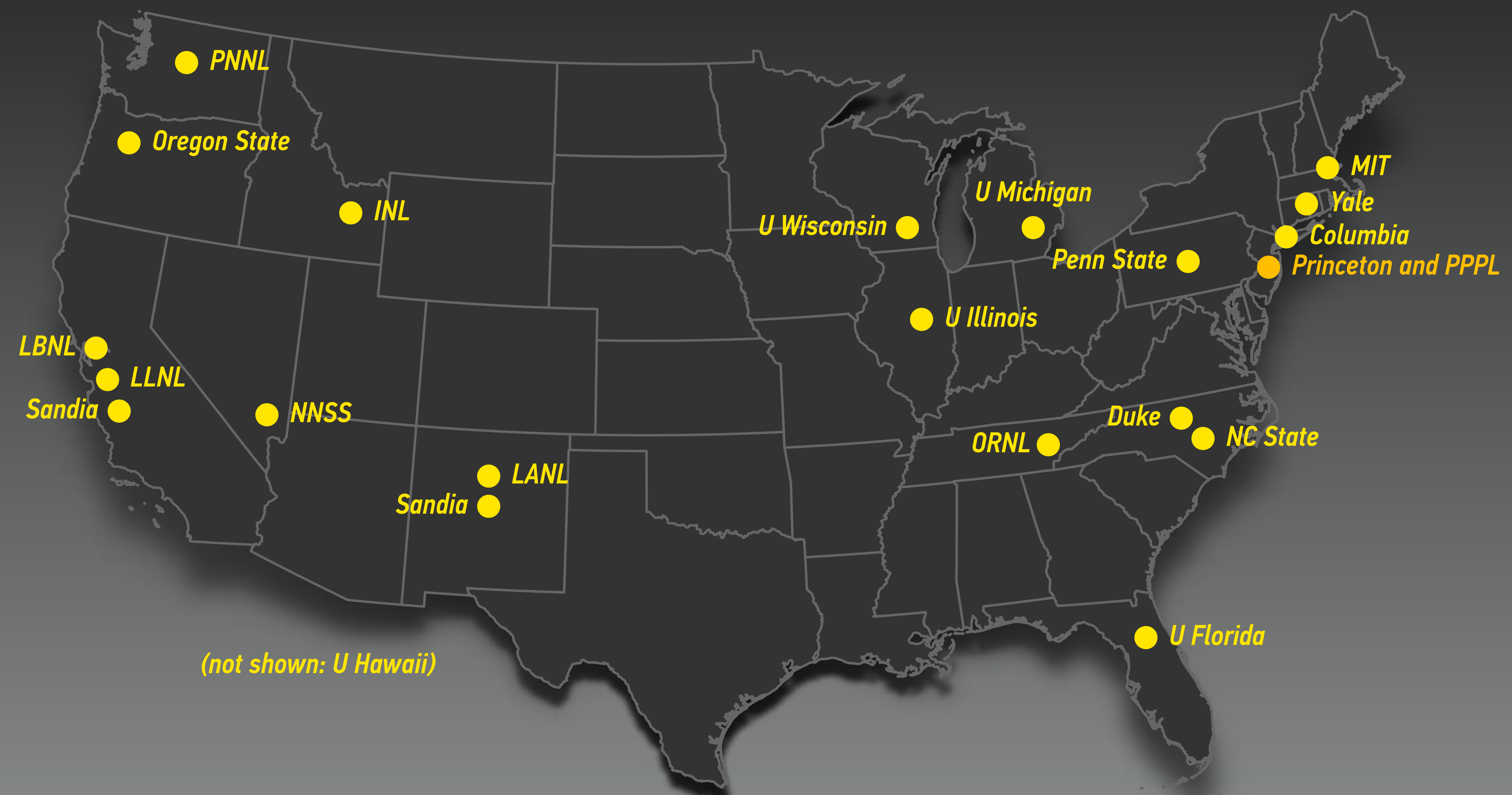
*Princeton University

**Princeton University and Princeton Plasma Physics Laboratory

Los Alamos National Laboratory, March 19, 2015

Revision 2z

CONSORTIUM FOR VERIFICATION TECHNOLOGY



Five-year project, funded by U.S. DOE, 13 U.S. universities and 9 national labs, led by U-MICH

Princeton participates in the research thrust on disarmament research
(and leads the research thrust of the consortium on policy)

BACKGROUND

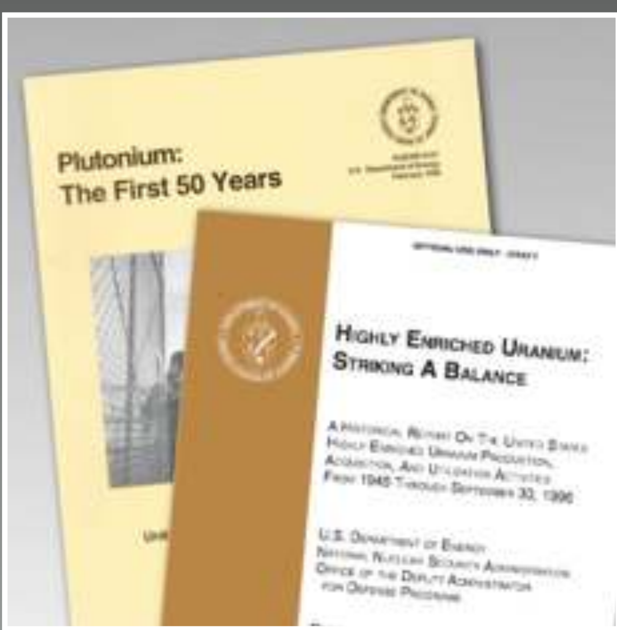
VERIFICATION CHALLENGES OF DEEP(ER) REDUCTIONS

WHAT IS NEW HERE?

THE CHALLENGES OF DEEP REDUCTIONS AND MULTILATERAL NUCLEAR ARMS CONTROL

NEW TREATIES MAY LIMIT TOTAL NUMBER OF WEAPONS

- Would then also include (non-deployed) weapons in storage
- Need to prepare for the transition from bilateral to multilateral nuclear arms control agreements



NEW TREATIES MAY REQUIRE BASELINE DECLARATIONS

- Applies to both nuclear warhead and fissile material inventories
- How to bring in countries that currently consider these numbers sensitive?

Source: Paul Shambroom (top) and U.S. Department of Energy (bottom)

WHAT IS TO BE VERIFIED?

VERIFICATION CHALLENGES OF NUCLEAR DISARMAMENT AT LOW NUMBERS

CORRECTNESS OF DECLARATIONS

- Warhead Counting

  Verify that numerical limit of declared items is not exceeded

- Warhead Authentication

  Verify authenticity of warheads prior to dismantlement

COMPLETENESS OF DECLARATIONS

- How to make sure that no covert warheads exist outside the verification regime?

Also (very) important, but not discussed here

Source: U.S. Department of Energy (top) and U.S. Department of Defense, www.defenseimagery.mil (bottom)

WHERE WE ARE COMING FROM

MOTIVATION BEHIND OUR PROJECT/RESEARCH

OUR GENERAL APPROACH

TEMPLATE-MATCHING (using active neutron interrogation)

More difficult to implement than attribute approach,
but also more robust against important diversion scenarios

Needs “golden warheads” to generate templates (reference signatures)

ZERO-KNOWLEDGE PROTOCOL

Can prove that a statement is true without revealing why it is true

If successfully implemented, no requirement for “engineered” information barrier

Robust against “curious verifier”

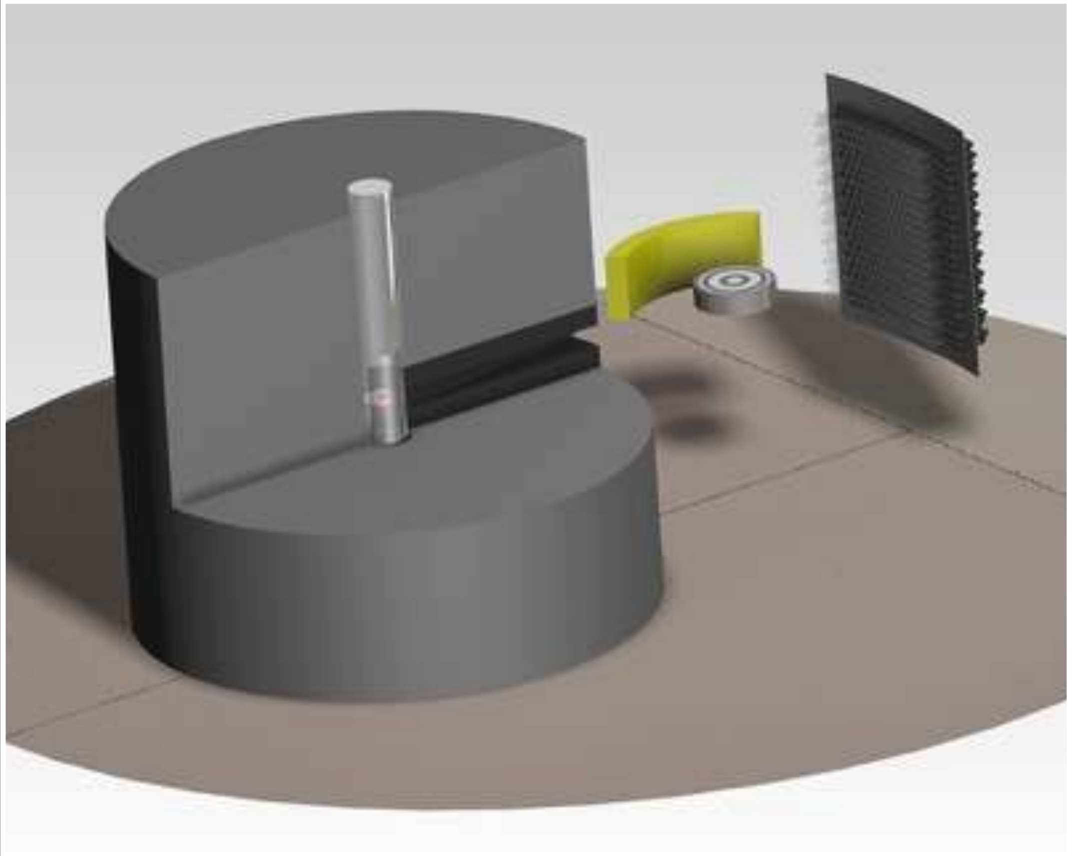
NON-ELECTRONIC DETECTORS

Electronic hardware and software used for detectors and/or information barriers
are hard to certify and authenticate

Technologies based on non-electronic detection and storage may offer important advantages

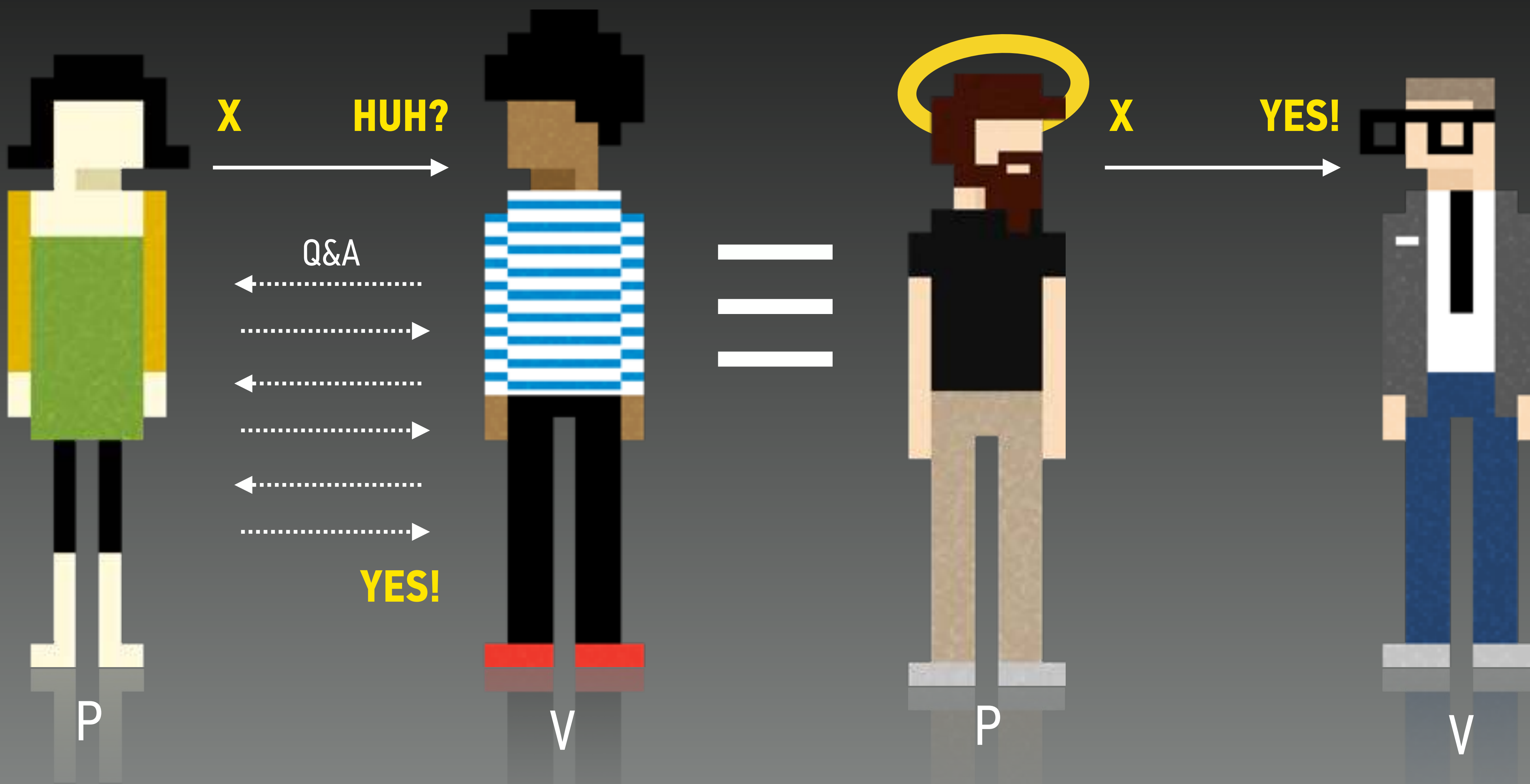
PRINCETON / GLOBAL ZERO WARHEAD VERIFICATION PROJECT

Princeton Plasma Physics Laboratory



Experimental setup
(currently under construction)

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

O. Goldreich, S. Micali, A. Wigderson, “How to Play ANY Mental Game,” 19th Annual ACM Conference on Theory of Computing, 1987
Graphics adapted from O. Goldreich, *Foundations of Cryptography,* Cambridge University Press, 2001; and eightbit.me

“NUMBER OF MARBLES IN A CUP”

Peggy (“the prover”) has two small cups each containing the same number of marbles. She wants to prove to Victor (“the verifier”) that both cups contain the same number of marbles without revealing to him what this number is.

BUBBLE DETECTORS OFFER A WAY TO IMPLEMENT THIS PROTOTOCL

AND AVOID DETECTOR-SIDE ELECTRONICS

Commercial bubble detectors (BTI Technologies)

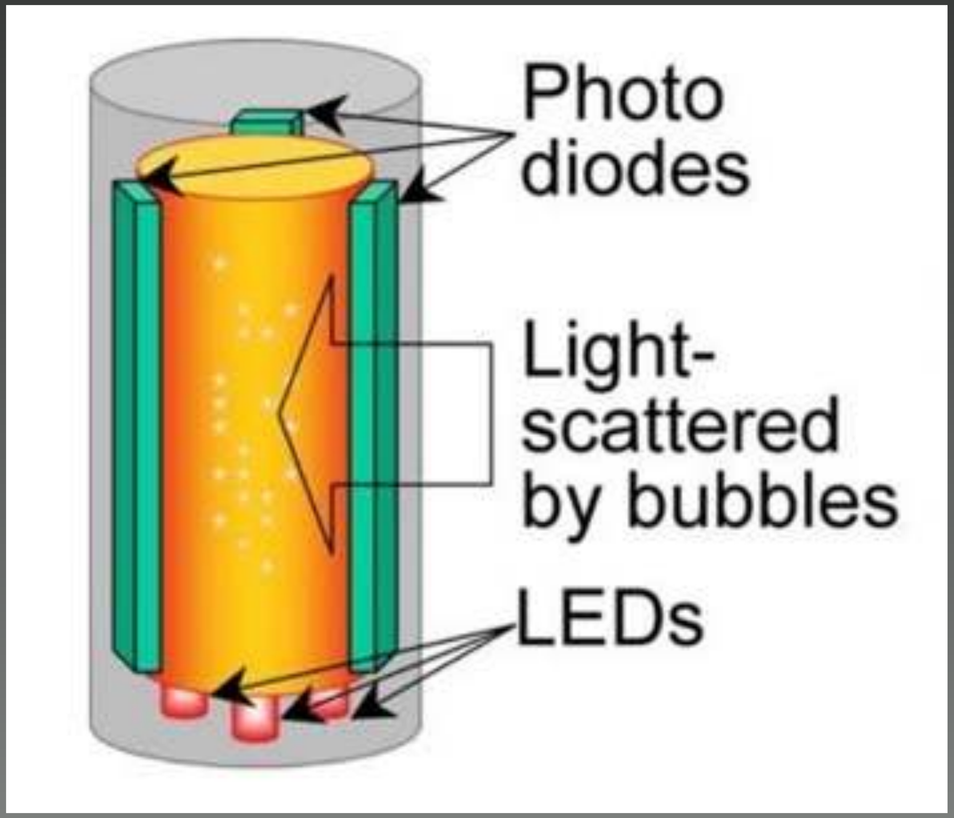
Optical readout with camera

Detectors with different neutron-energy thresholds (no cutoff, 500 keV, 1 MeV, 10 MeV) allow measurements that are sensitive to different diversion scenarios

BUBBLE DETECTORS OFFER A WAY TO IMPLEMENT THIS PROTOTOCL

AND AVOID DETECTOR-SIDE ELECTRONICS

Commercial bubble detectors (BTI Technologies)



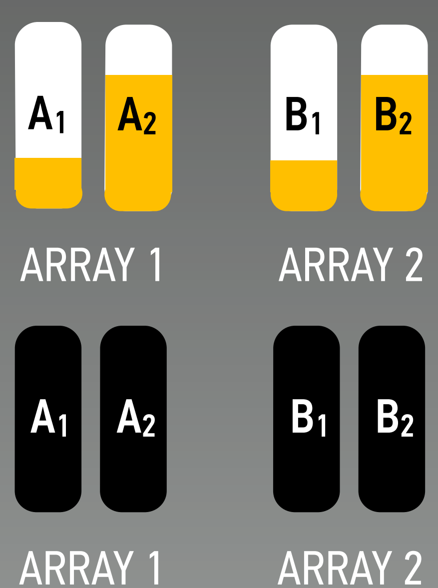
Optical readout with LEDs and photodiodes (Yale)

Detectors with different neutron-energy thresholds (no cutoff, 500 keV, 1 MeV, 10 MeV) allow measurements that are sensitive to different diversion scenarios

PROPOSED HARDWARE IMPLEMENTATION OF A ZERO-KNOWLEDGE PROTOCOL FOR NUCLEAR WARHEAD VERIFICATION

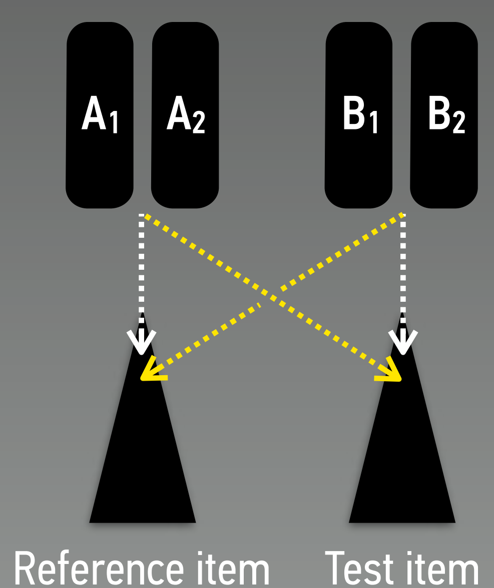
1

Host secretly preloads arrays of bubble detectors with "negative" radiograph of the reference item



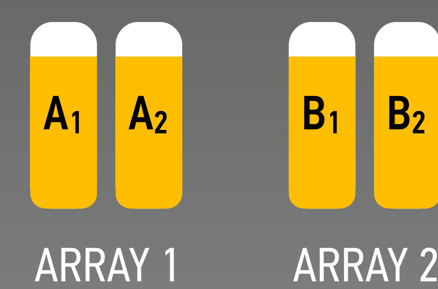
2

Inspector randomly chooses, which preloaded array to use on which item



3

After interrogation, inspector verifies that detectors in arrays contain the same bubble count



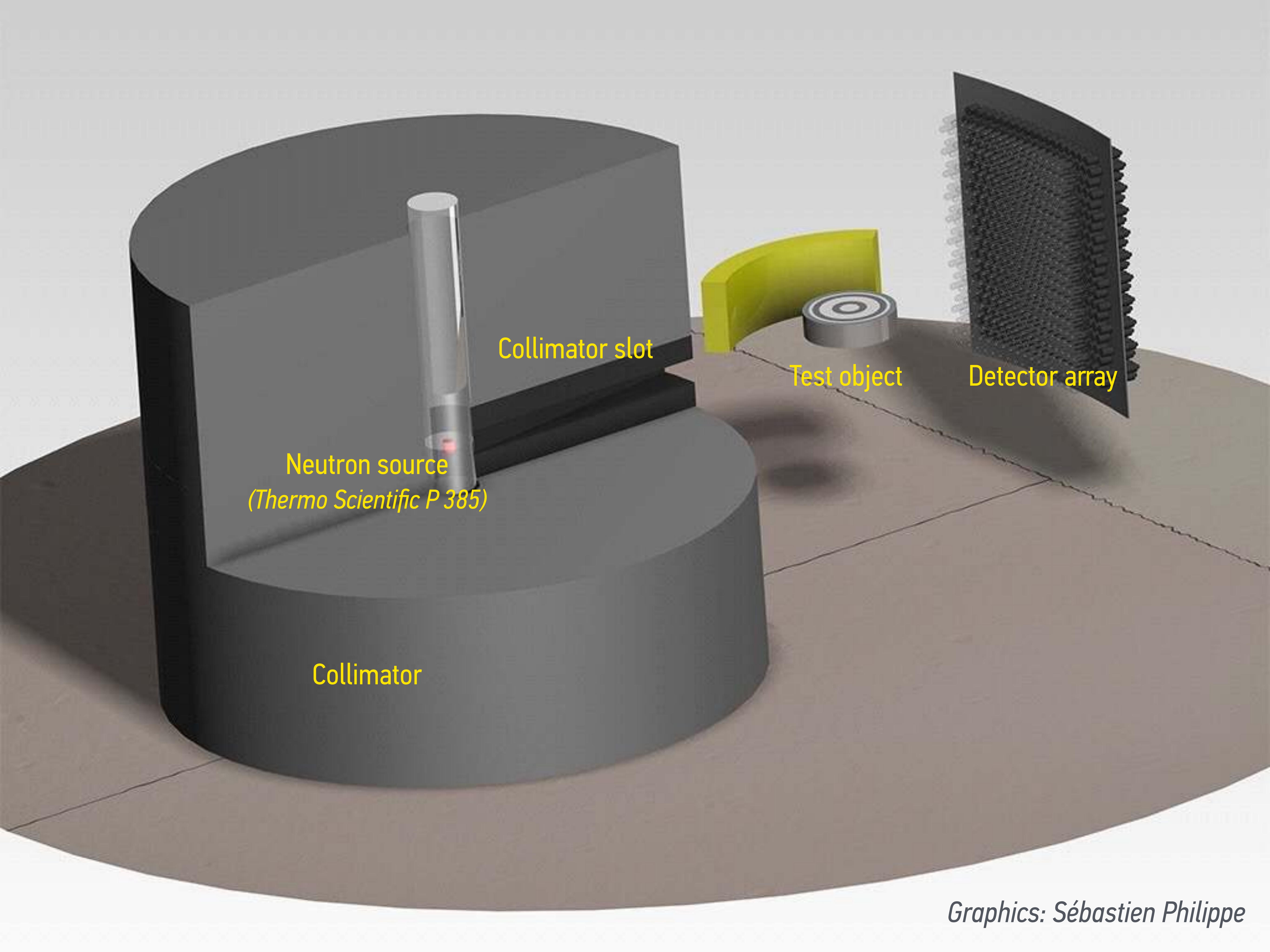
50% confidence after 1st round

...

95% confidence after 5th round

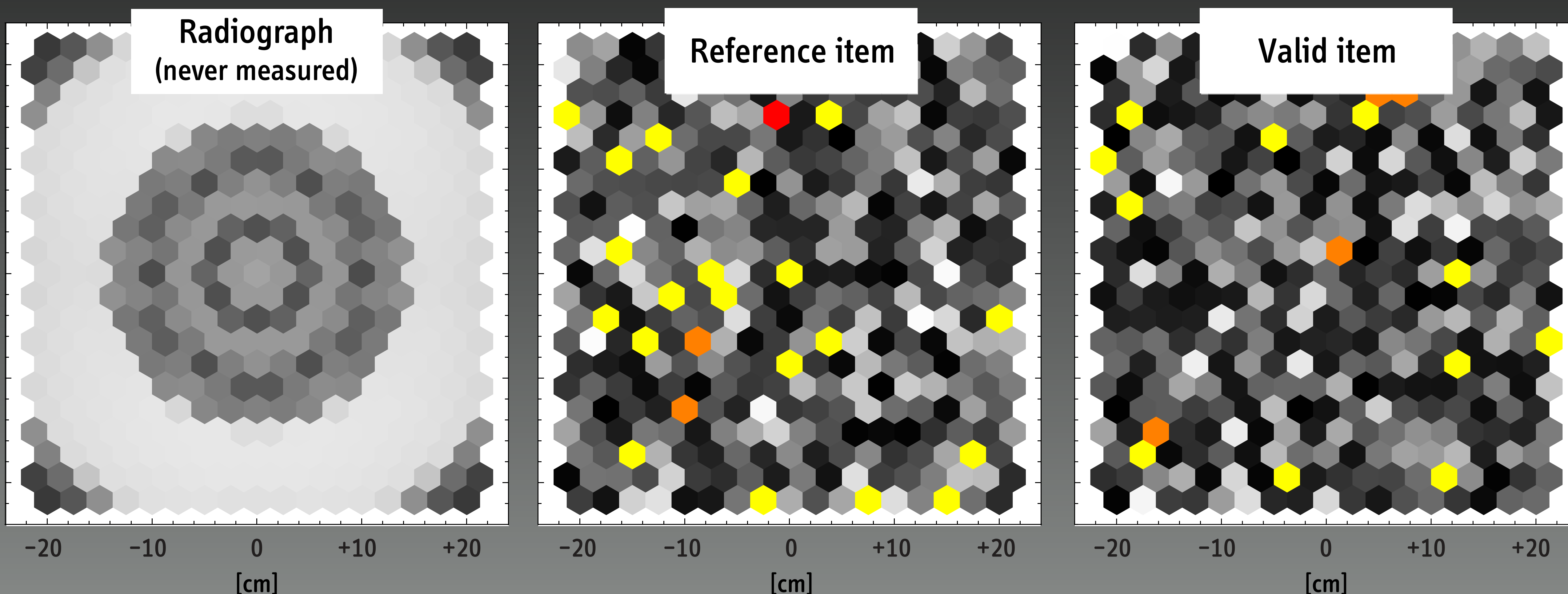
RESULTS

RADIOGRAPHY WITH 14-MeV NEUTRONS


Collimator slot
Test object
Detector array
Neutron source
(Thermo Scientific P 385)
Collimator
Graphics: Sébastien Philippe

ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS



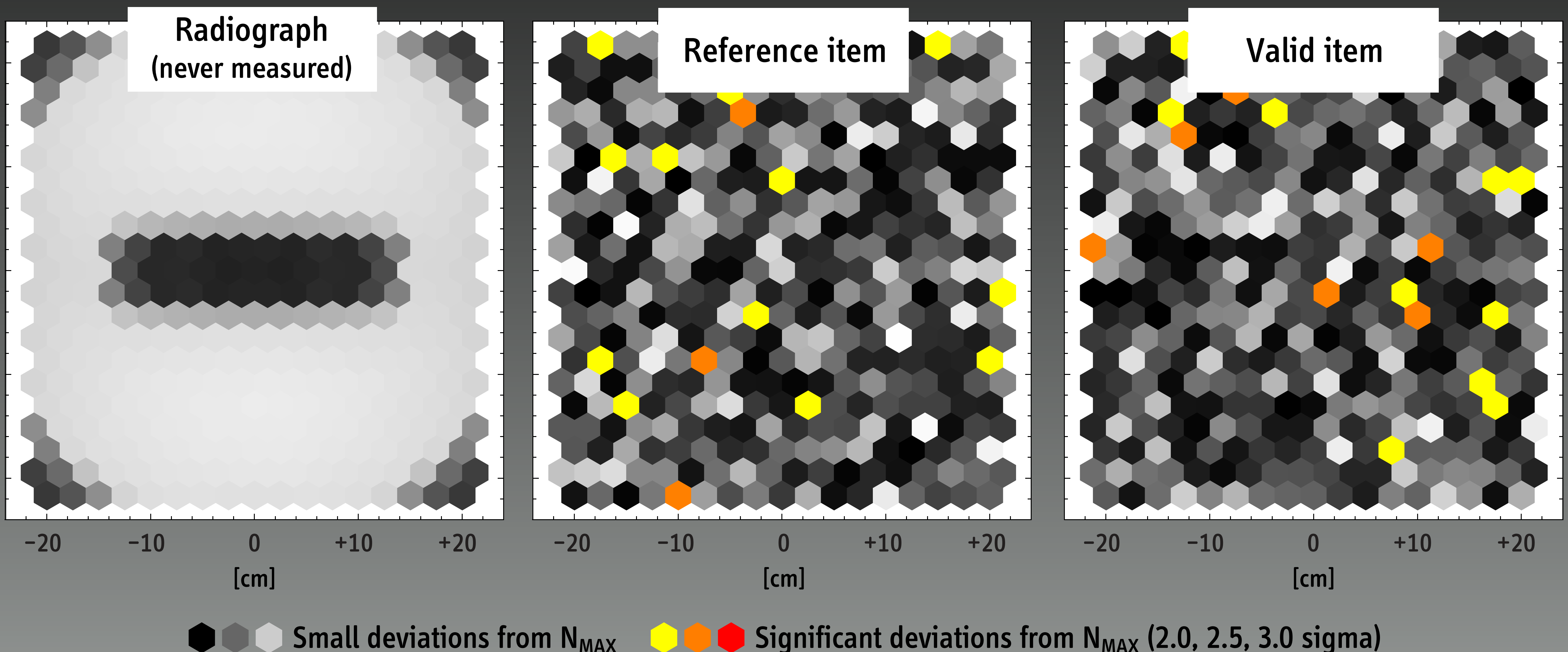
Small deviations from N_{MAX} Significant deviations from N_{MAX} (2.0, 2.5, 3.0 sigma)

Simulated data from MCNP calculations; neutron detection energies > 10 MeV; N(max) = 5,000

A. Glaser, B. Barak, R. J. Goldston, “A Zero-knowledge Protocol for Nuclear Warhead Verification,” *Nature,* 510, 26 June 2014, 497–502

ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS



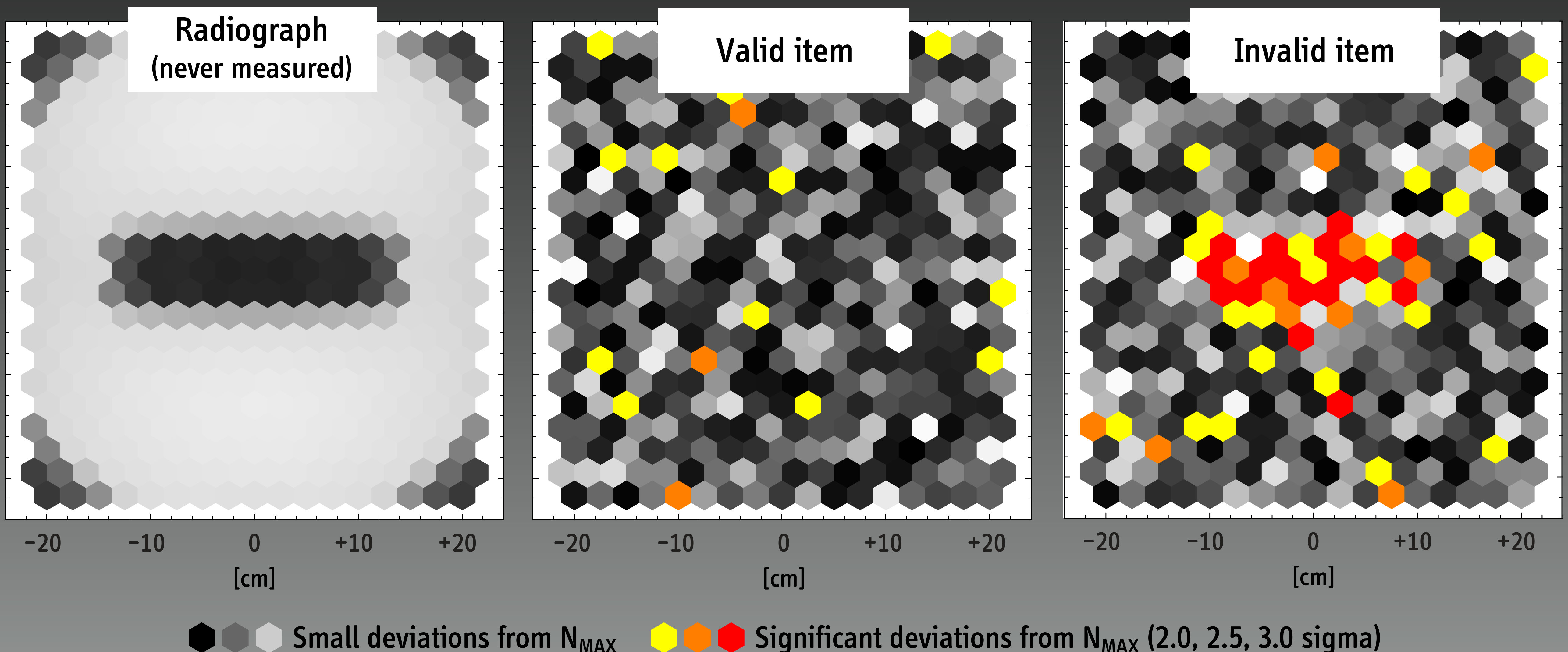
Simulated data from MCNP calculations; neutron detection energies > 10 MeV; N(max) = 5,000

A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502

ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS

(Tungsten rings replaced by lead rings)

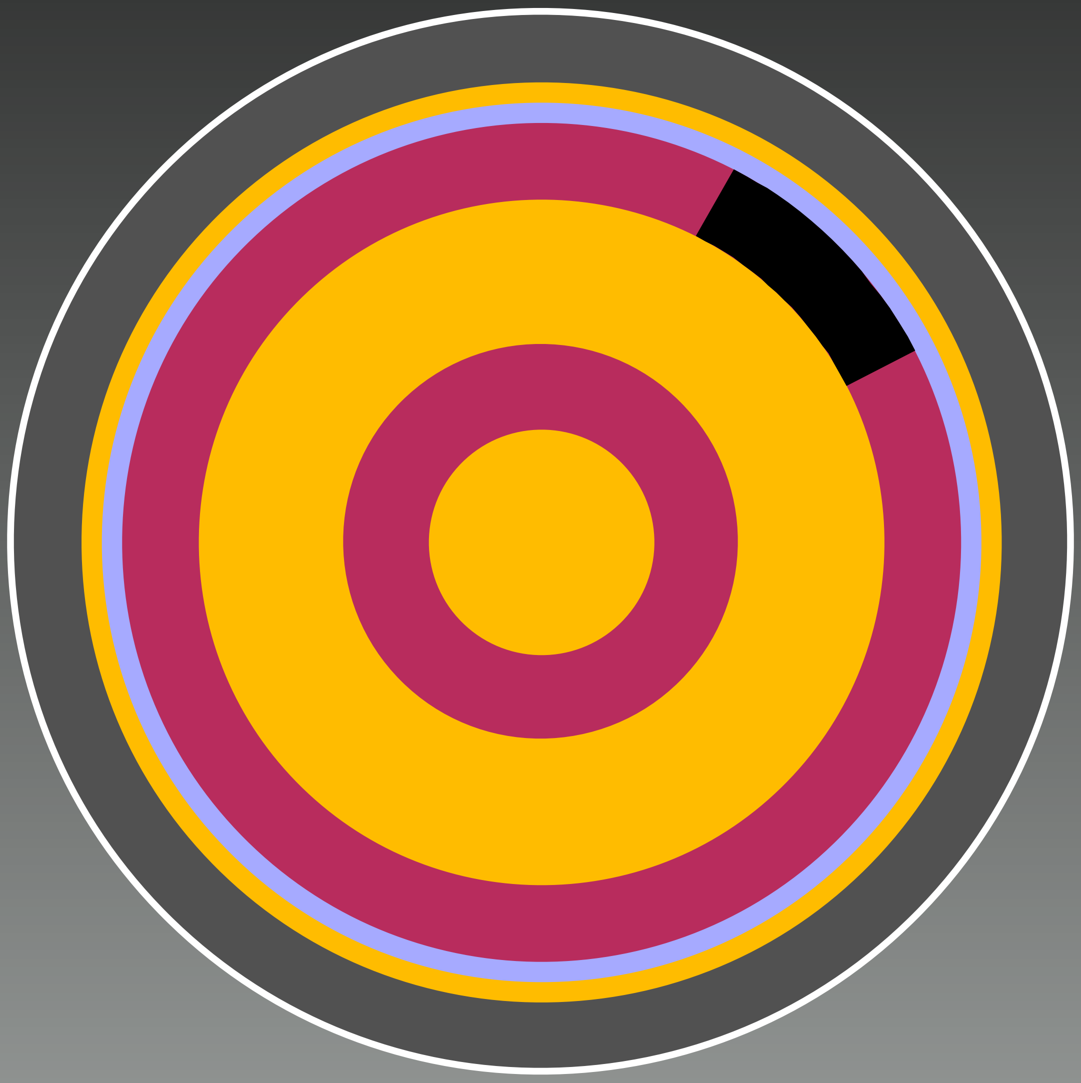


Simulated data from MCNP calculations; neutron detection energies > 10 MeV; N(max) = 5,000

A. Glaser, B. Barak, R. J. Goldston, “A Zero-knowledge Protocol for Nuclear Warhead Verification,” *Nature,* 510, 26 June 2014, 497–502

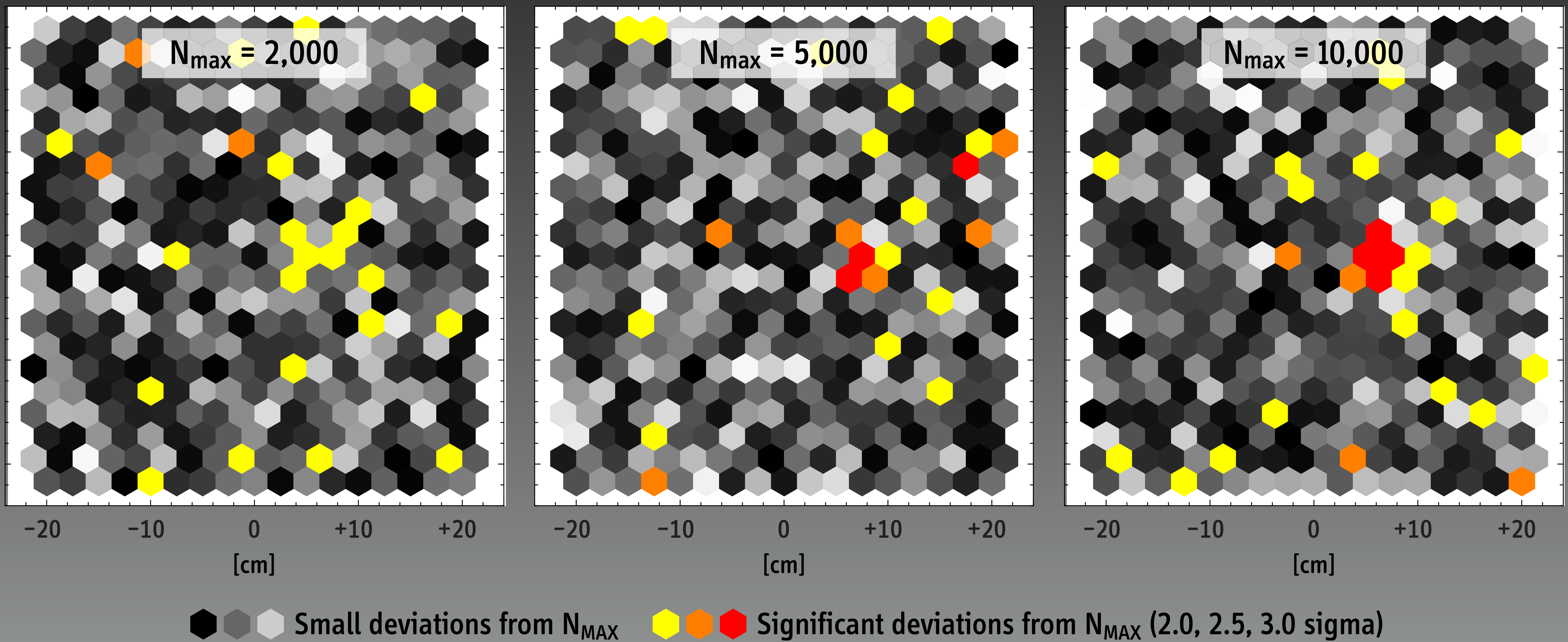
LOCAL TUNGSTEN DIVERSION

36-DEGREE SEGMENT OF OUTER TUNGSTEN RING (543 GRAMS, 7% OF TOTAL TUNGSTEN)



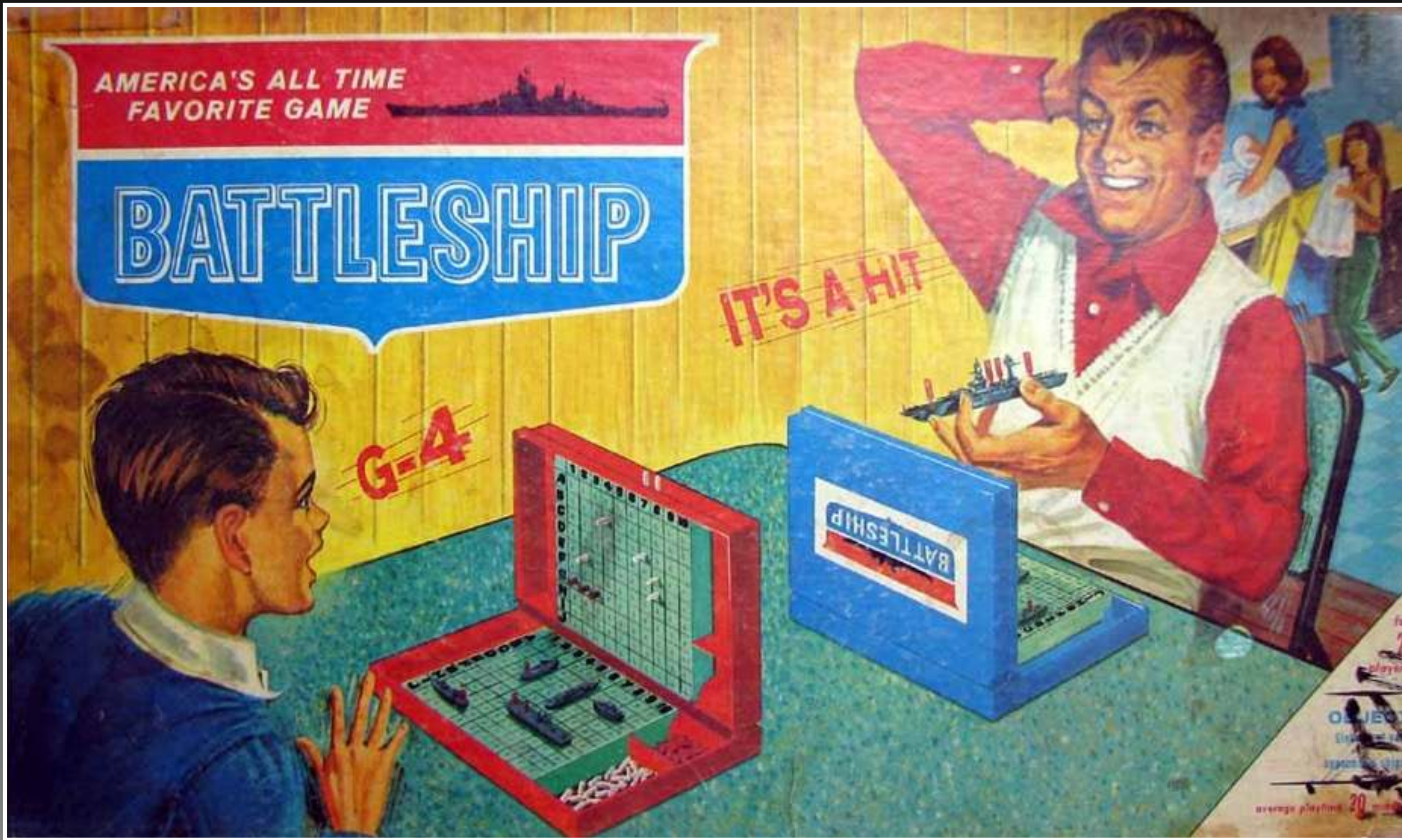
ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS



543 grams of tungsten removed from outer ring of test object; simulated data from MCNP calculations; neutron detection energies > 10 MeV

A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502



Source: Milton Bradley

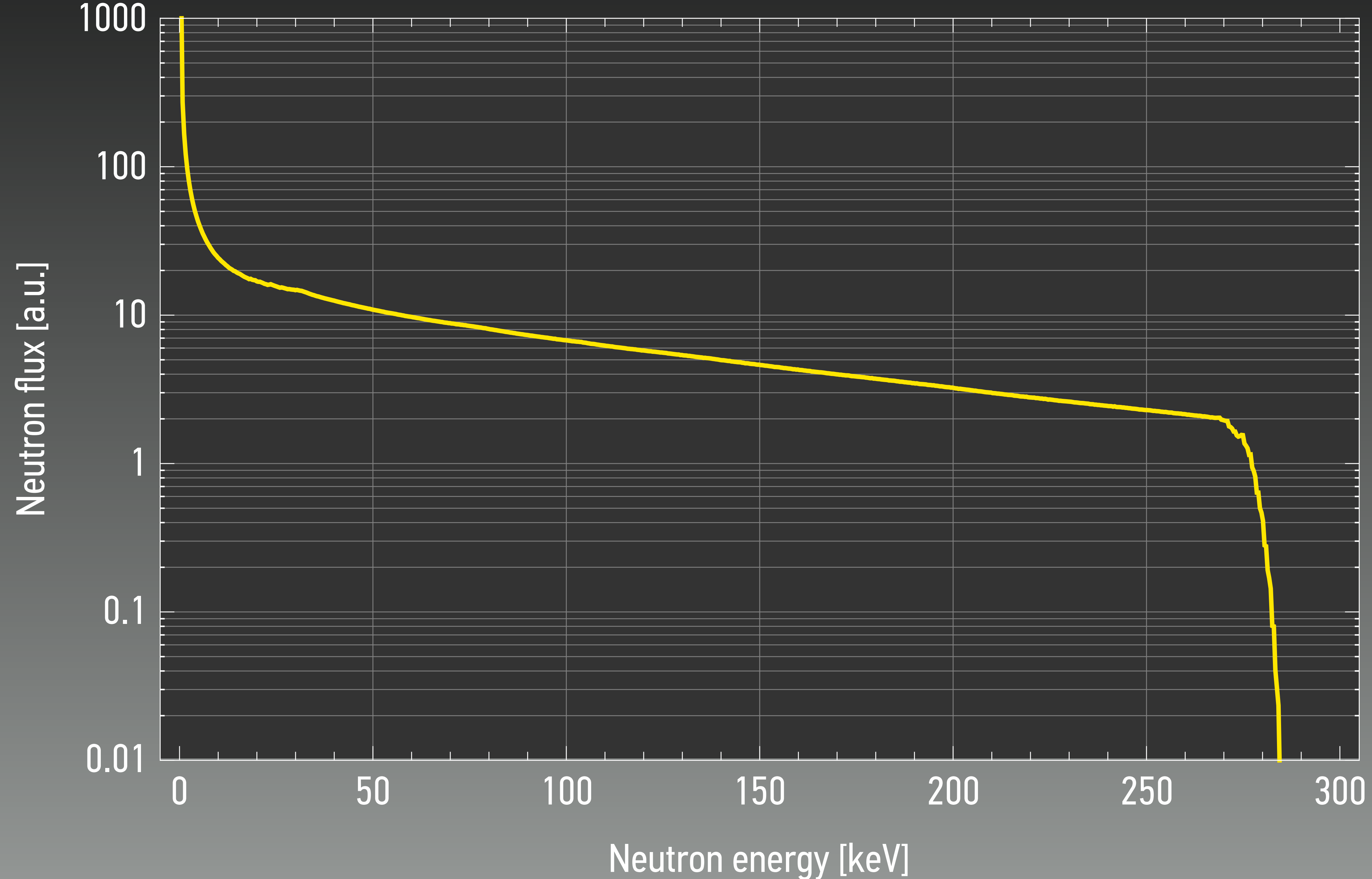
“TWO-COLOR INTERROGATION”

INTERROGATION WITH NEUTRONS FROM (p-^{7}Li) REACTION

(tuned to ~300 keV energy cutoff)

SIMULATED NEUTRON SPECTRUM

FROM PROTON-LITHIUM DRIVEN NEUTRON SOURCE IN COLLIMATOR



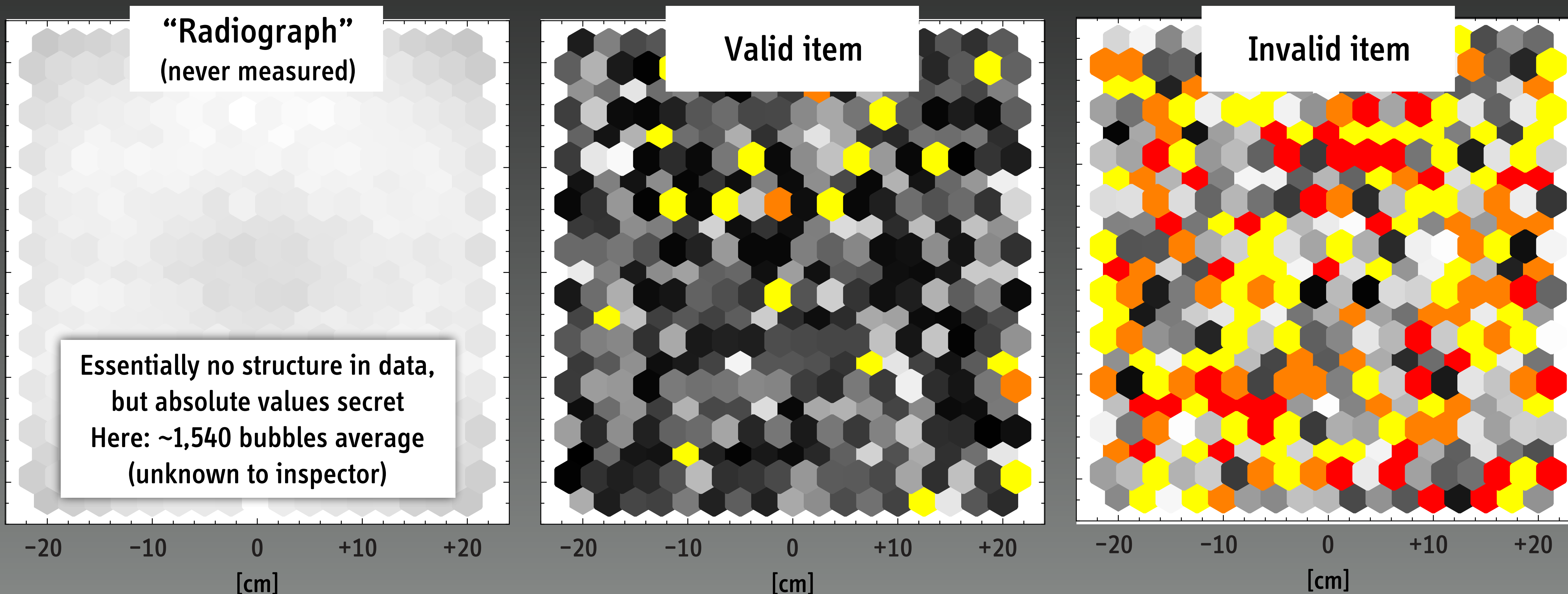
(In forward direction, measured at collimator exit, MCNP6 simulations)

BARE PLUTONIUM SPHERE

8.00 cm DIAMETER SPHERE, WEAPON-GRADE PLUTONIUM

Test item based on BeRP ball, see J. Mattingly and D. J. Mitchell, *Applied Radiation and Isotopes,* 70 (2012), 1136–1140

(Isotopic shift from 93.7% to 81.2% Pu-239)



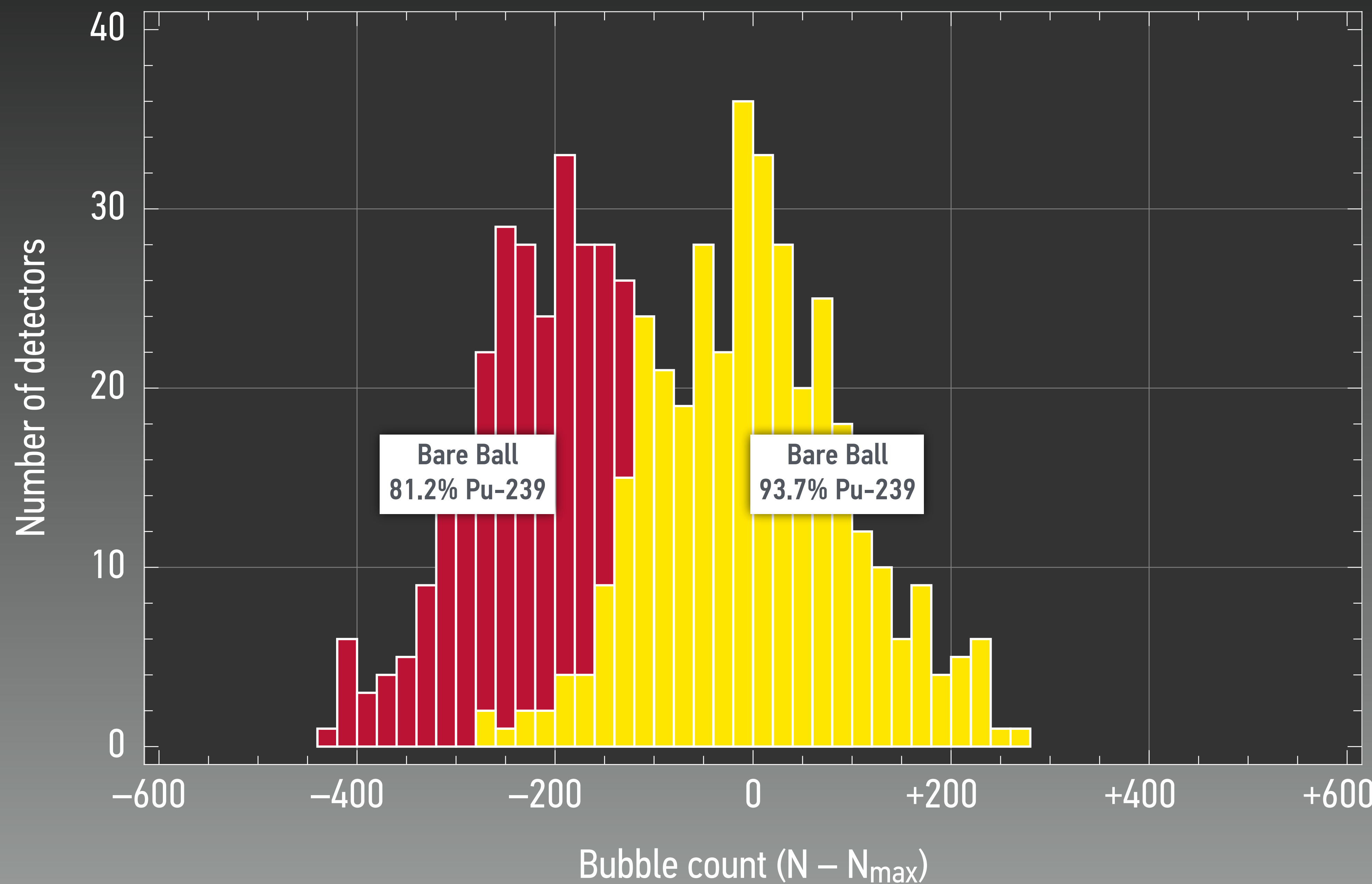
Small deviations from N_{MAX} Significant deviations from N_{MAX} (2.0, 2.5, 3.0 sigma)

Simulated data from MCNP6 calculations, neutron detection energies > 500 keV
N(max) = 10,000, i.e., 6–7 times higher than actual values from test item

BARE PLUTONIUM SPHERE

8.00 cm DIAMETER SPHERE, WEAPON-GRADE PLUTONIUM

Test item based on BeRP ball, see J. Mattingly and D. J. Mitchell, *Applied Radiation and Isotopes,* 70 (2012), 1136–1140



MCNP6 simulations, N(max) = 10,000

WHAT IF SOMETHING GOES TERRIBLY WRONG?

Possible Fail-Secure Mechanisms for ZKP Verification

FAIL-SECURE DATA VERIFICATION AND RELEASE

If inspection system works properly and items are placed correctly,
no information in signal or noise

But what if something went wrong during inspection (unknown to host)?

Problem with inspection system and/or problem with setup (alignment, detector location, etc.)

Host wants to make sure measured data does not contain
any information (besides N_{max} and its Poisson noise)

Challenge: How to design a protocol that allows the host to screen the data
without the inspector losing trust in the integrity of the data

Proposed solution: Data commitment

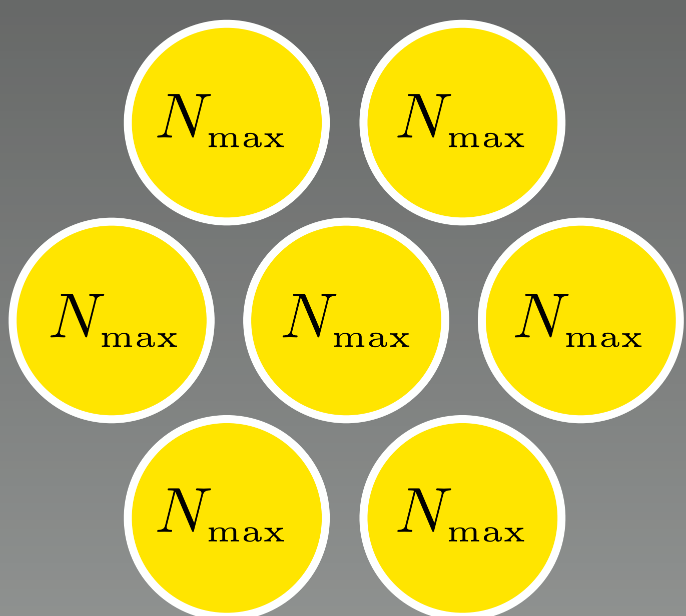
COMMITMENT SCHEME 1

“DATA ASSURANCE”

1

Detectors after inspection

No information in data or noise if inspection successful



2

Detector information is “committed” (using non-electronic medium)

For example, by (blindly) taking photographs of the detectors (without developing the film)

3

Host analyzes the detectors in private to confirm that no residual information is present

Once detectors are released by host, the inspector is allowed to read out the detectors (with agreed method) and to compare against committed data (e.g. on photographs)

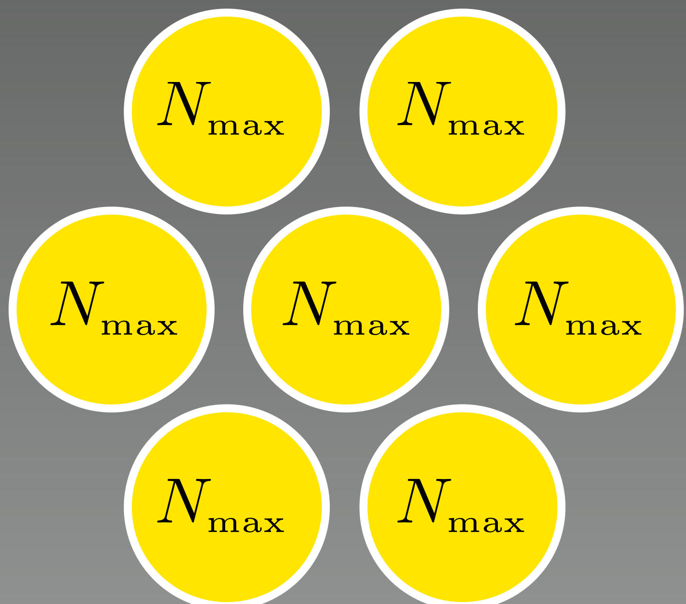
COMMITMENT SCHEME 2

"DATA SPLITTING"

1

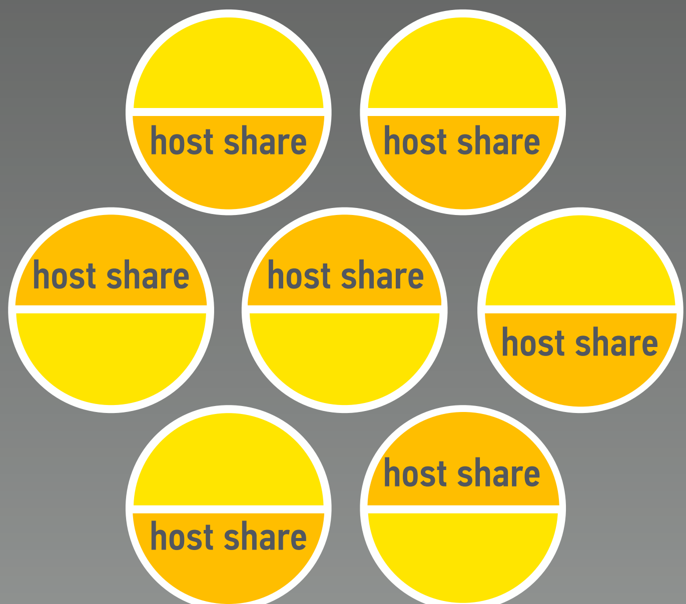
Detectors after inspection

No information in data or noise if inspection successful



2

Detector information is divided (at host's discretion)



3

Host analyzes her share of the detectors in private to confirm that no residual information is present

Once the host is satisfied with the data in her share, the inspector is allowed to read out the data in his share (with agreed method)

TO BE CONTINUED

ACKNOWLEDGEMENTS

PRINCETON

Charles Gentile
Robert J. Goldston
Sébastien Philippe

ELSEWHERE

Boaz Barak (Microsoft Research New England)
Francesco d'Errico (Yale University)
Margarita Gattas-Sethi (Yale University)
Moritz Kütt (Technische Universität Darmstadt)

RESEARCH SUPPORTED BY

Global Zero
MacArthur Foundation
Carnegie Corporation of New York
U.S. Department of State
National Nuclear Security Administration, U.S. Department of Energy