HOW TO KEEP A SECRET

NEW APPROACHES TO TRUSTED RADIATION MEASUREMENTS FOR NUCLEAR WARHEAD VERIFICATION

Alexander Glaser

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

Technische Universität Darmstadt, 8. Juli 2016

Revision 1

CURRENT AREAS OF RESEARCH

nuclearfutures.princeton.edu

Nuclear Energy and Nuclear Proliferation

Can one safely expand the use of nuclear power without increasing the risk of nuclear proliferation ?

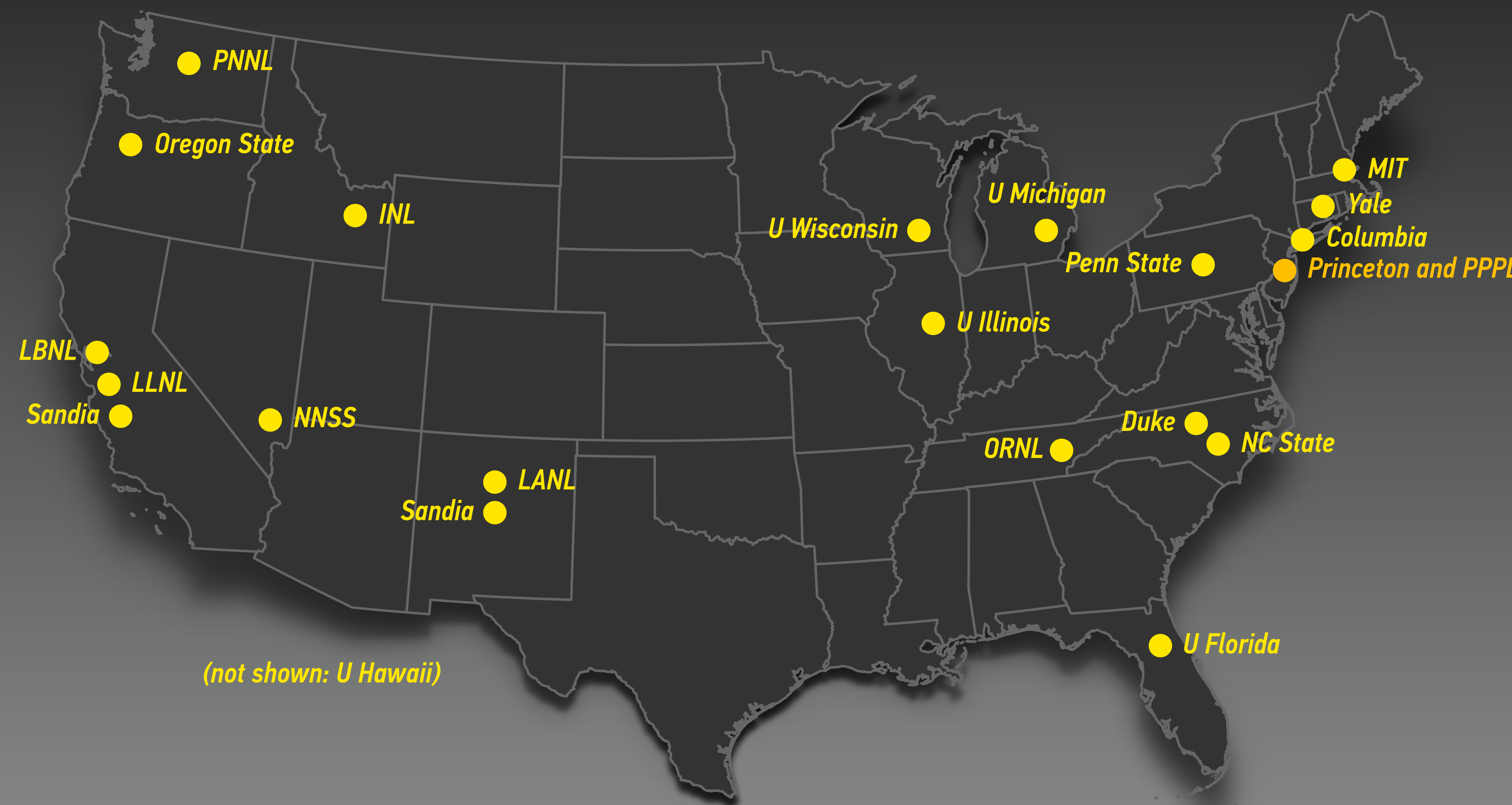
Nuclear Energy and Climate Change

Are there new reactor technologies that could be potential "game changers" for nuclear power ?

Verification of Nuclear Arms Control Treaties

Can one dismantle an atomic bomb without learning anything about its design ?

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)

INTERNATIONAL PARTNERSHIP

FOR NUCLEAR DISARMAMENT VERIFICATION

Established in 2015; currently 26 participating countries (including Germany)

Working Group One: “Monitoring and Verification Objectives” (chaired by Italy and the Netherlands)

Working Group Two: “On-Site Inspections” (chaired by Australia and Poland)

Working Group Three: “Technical Challenges and Solutions” (chaired by Sweden and the United States)

www.state.gov/t/avc/ipndv

RELEVANT NUCLEAR ARMS CONTROL TREATIES

NUCLEAR NON-PROLIFERATION TREATY

Bans the acquisition of nuclear weapons by non-weapon states and commits the five weapon states to nuclear disarmament; verified by IAEA safeguards

COMPREHENSIVE TEST BAN TREATY

Bans all nuclear explosions in all environments and would be verified by extensive verification mechanisms (International Monitoring System, CTBTO)

FISSILE MATERIAL (CUTOFF) TREATY

At a minimum, treaty would ban fissile material production for weapons purposes; Issue about treaty scope: Would it also cover existing stocks?

NEXT-GENERATION NUCLEAR DISARMAMENT TREATIES

Agreements that place limits on total number of nuclear warheads in arsenals would pose qualitatively new verification challenges

CONFIRMING THE AUTHENTICITY OF A NUCLEAR WARHEAD

(WHILE LEARNING NOTHING ABOUT IT)

(START CALIBRATION AND/OR TEMPLATE ACQUISITION)

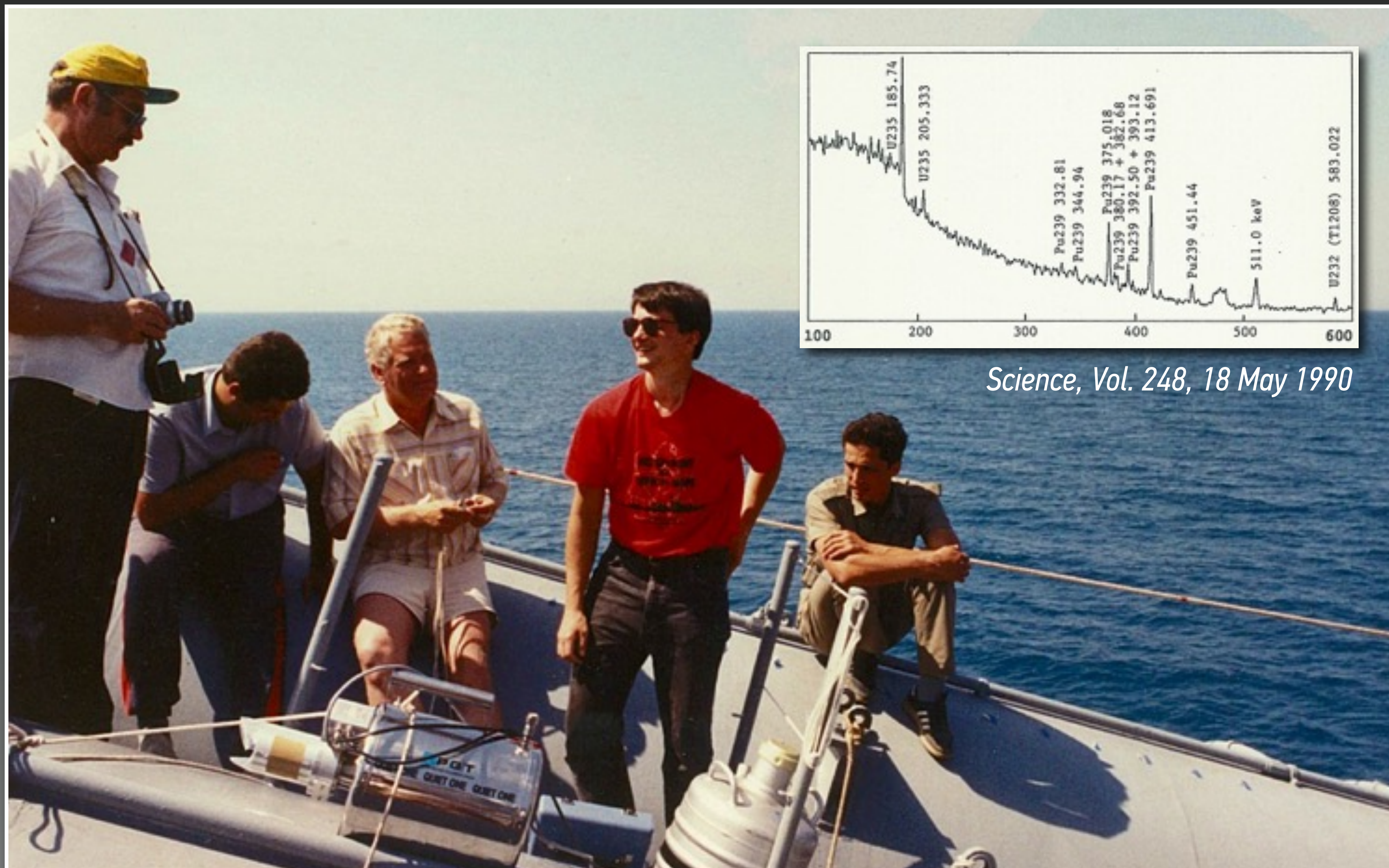
THOUSANDS OF NUCLEAR WEAPONS

ARE CURRENTLY NON-DEPLOYED (i.e., IN RESERVE OR AWAITING DISMANTLEMENT)

W87/Mk-21 Reentry Vehicles in storage, Warren Air Force Base, Cheyenne, Wyoming
Photo courtesy of Paul Shambroom, www.paulshambroom.com

NUCLEAR WEAPONS HAVE UNIQUE SIGNATURES

BUT THEY ARE SENSITIVE AND CANNOT BE REVEALED TO INSPECTORS

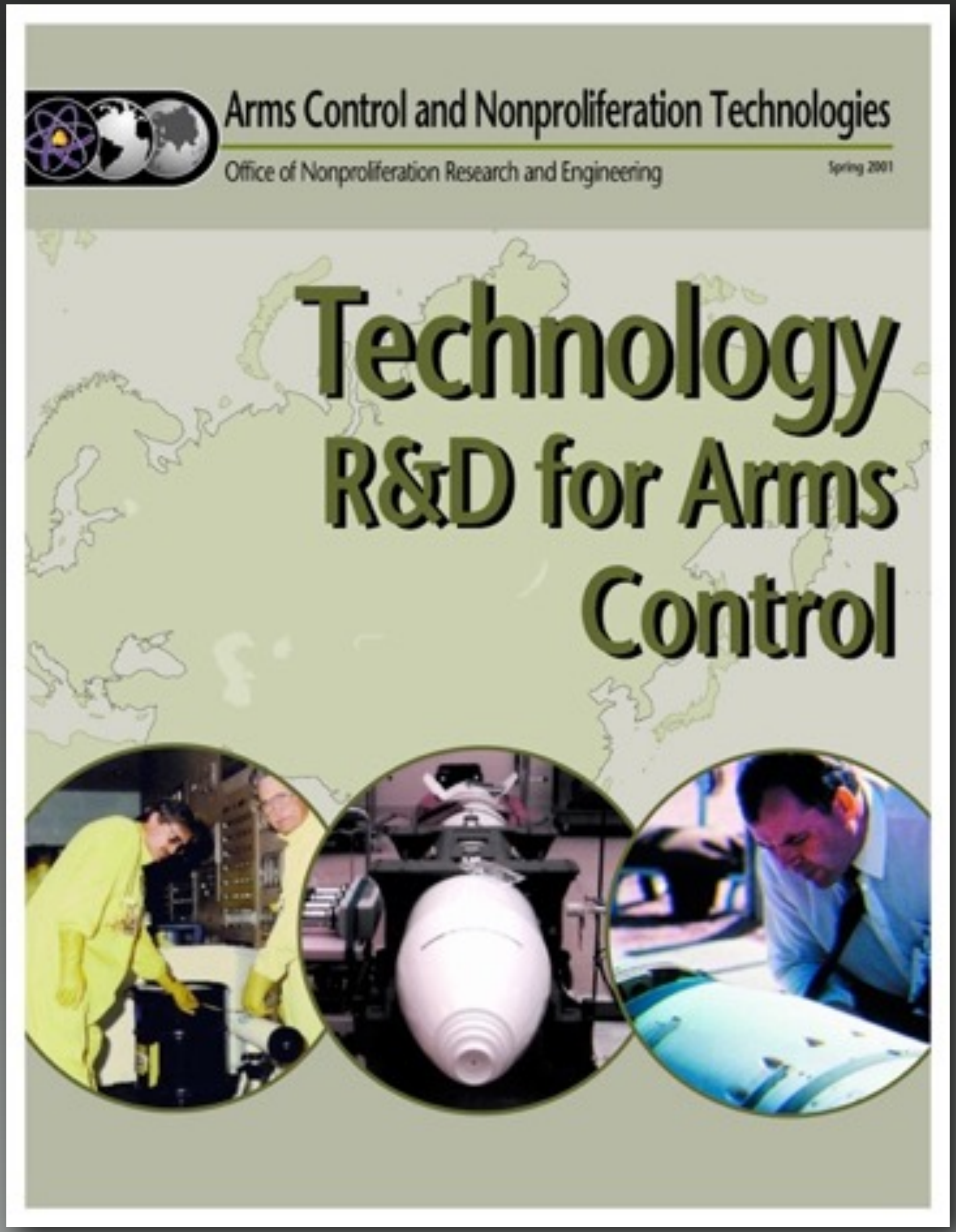


Science, Vol. 248, 18 May 1990

U.S. Scientists on a Soviet Cruiser in the Black Sea, 1989

NUCLEAR WARHEAD VERIFICATION

KEY CONCEPTS OF (PROPOSED) SYSTEMS



edited by D. Spears, 2001

ATTRIBUTE APPROACH

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

TEMPLATE APPROACH

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

INFORMATION BARRIERS

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

PREVENTING THE EXCHANGE OF SENSITIVE INFORMATION DURING A RADIATION MEASUREMENT

Trusted Information Barrier

Measure (but sanitize) sensitive information

“Hard” to authenticate and certify

Single-bit observation

Interactive Zero-knowledge Proof

Never measure sensitive information

“Easy” to authenticate and certify

More complex observation

S. Philippe, B. Barak, and A. Glaser, “Designing Protocols for Nuclear Warhead Verification”
56th Annual INMM Meeting, July 12-16, 2015, Indian Wells, California

WHY ARE WARHEAD INSPECTIONS SO HARD?

(AS SEEN FROM INSPECTOR'S PERSPECTIVE)

VERY LITTLE (IF ANY) INFORMATION ABOUT THE INSPECTED ITEM CAN BE REVEALED

Some information may be shared in advance, but no additional information during inspection

ADVERSARY/COMPETITOR HAS (DE FACTO) INFINITE RESOURCES

ADVERSARY/COMPETITOR MAY BE EXTREMELY MOTIVATED (TO DECEIVE INSPECTOR)

Stakes are very high (especially when the number of weapons drops below ~1,000)

HOST HAS LAST OWNERSHIP OF INSPECTION SYSTEM <u>BEFORE</u> THE MEASUREMENT

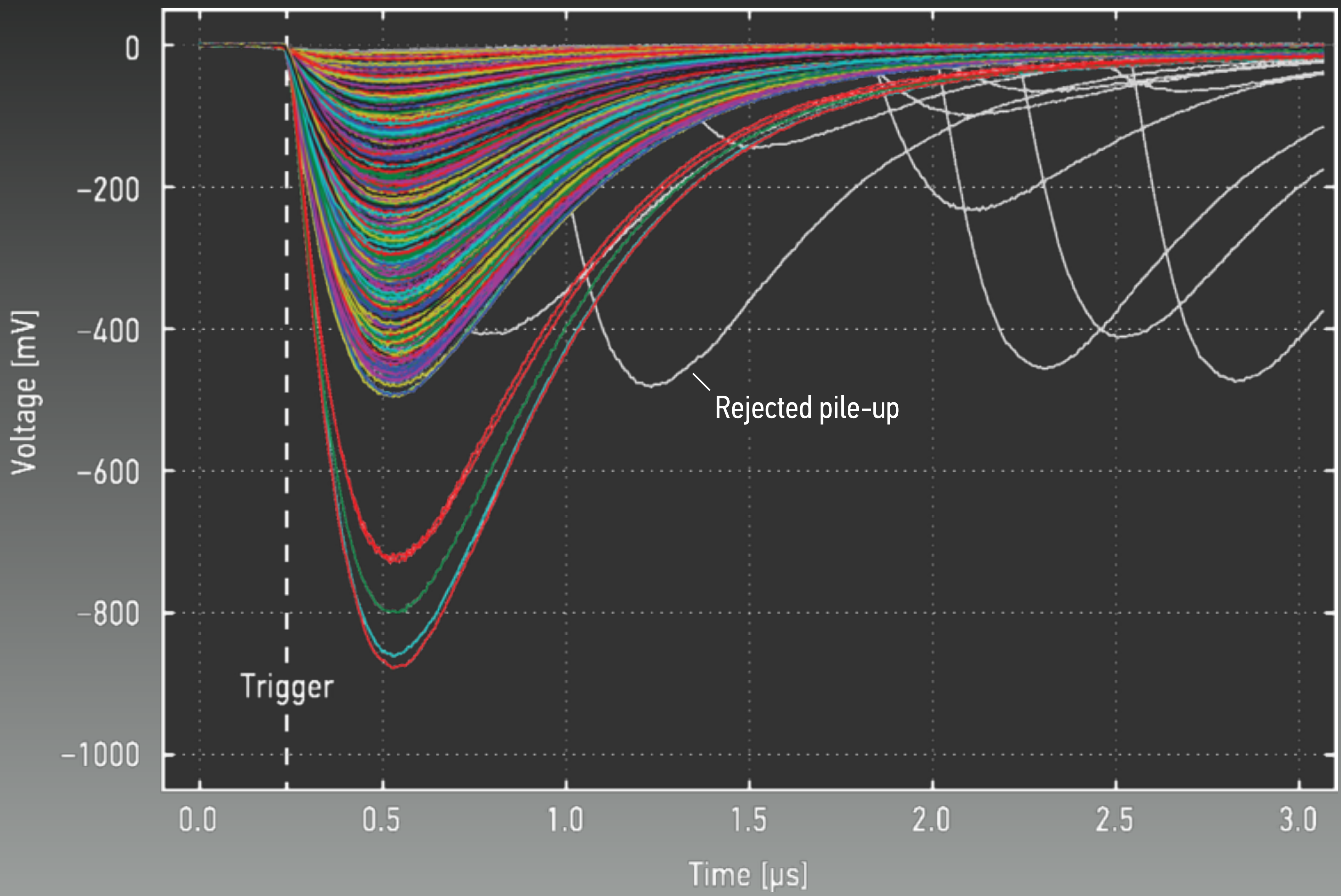
(and inspector never again has access to system <u>after</u> the measurement is complete)

WHILE WE ARE WAITING

PASSIVE GAMMA SPECTROSCOPY WITH INFORMATION BARRIER

INFORMATION BARRIER EXPERIMENTAL

VOLTAGE PULSES ACQUIRED BY THE RED PITAYA

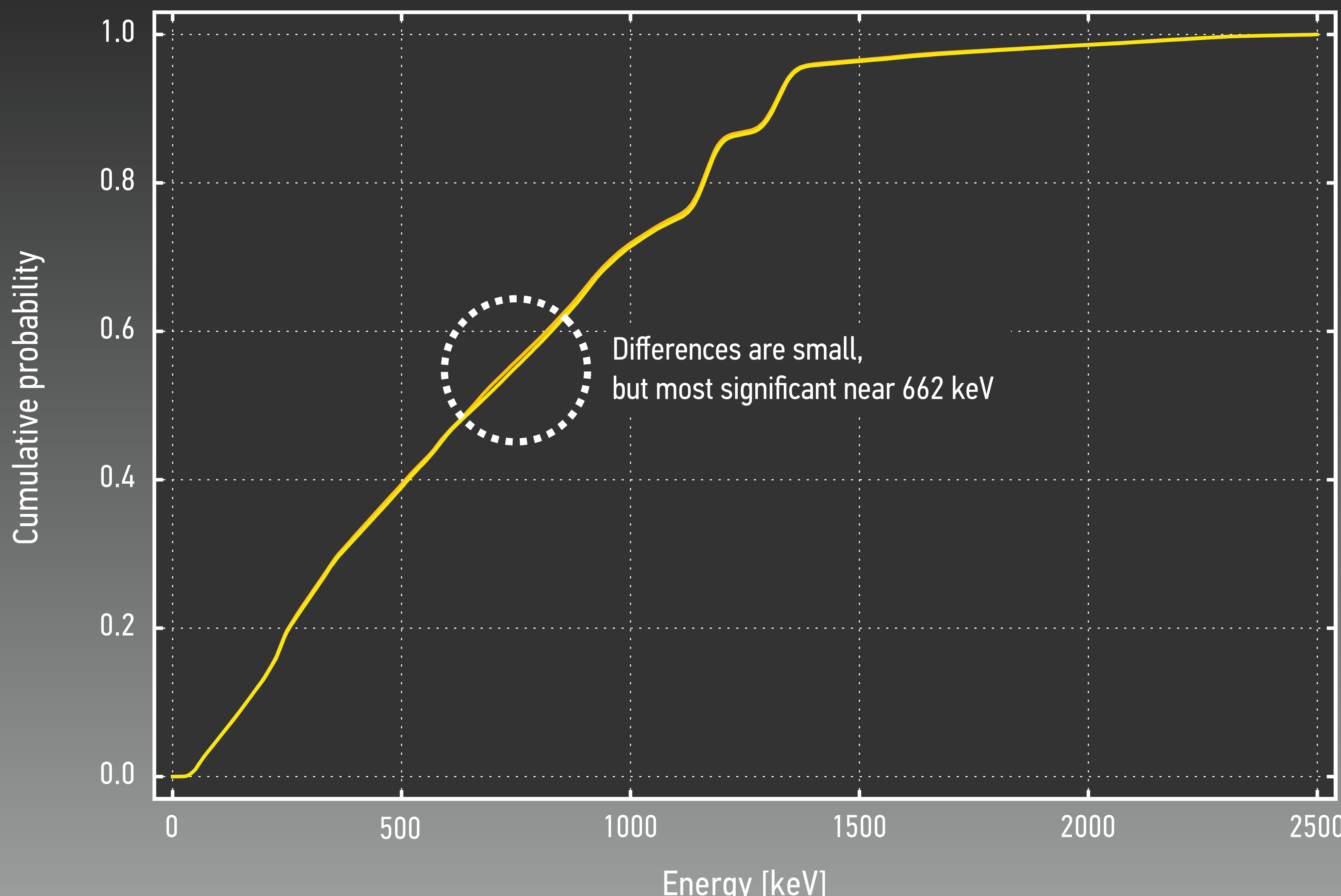


COMPARING RADIATION SPECTRA

(IBX WITH SODIUM-IODIDE DETECTOR, 60 SECONDS, ~175,000 counts)

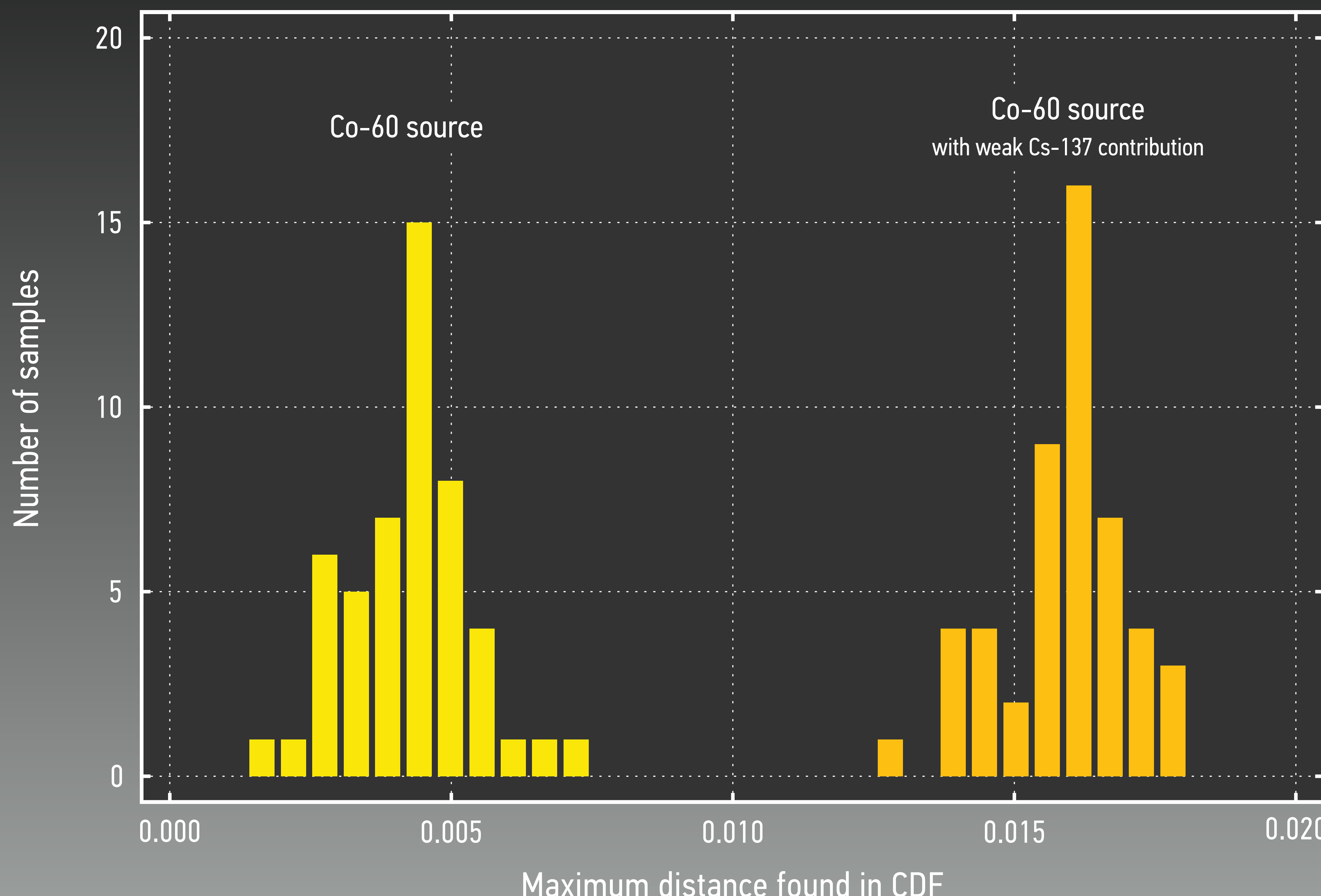
COMPARING RADIATION SPECTRA

(IBX WITH SODIUM-IODIDE DETECTOR, 60 SECONDS, ~175,000 counts)



COMPARING RADIATION SPECTRA

(IBX WITH SODIUM-IODIDE DETECTOR, 60 SECONDS, ~175,000 counts)



PREVENTING THE EXCHANGE OF SENSITIVE INFORMATION DURING A RADIATION MEASUREMENT

Trusted Information Barrier

Measure (but sanitize) sensitive information

“Hard” to authenticate and certify

Single-bit observation

Interactive Zero-knowledge Proof

Never measure sensitive information

“Easy” to authenticate and certify

More complex observation

S. Philippe, B. Barak, and A. Glaser, “Designing Protocols for Nuclear Warhead Verification”
56th Annual INMM Meeting, July 12-16, 2015, Indian Wells, California

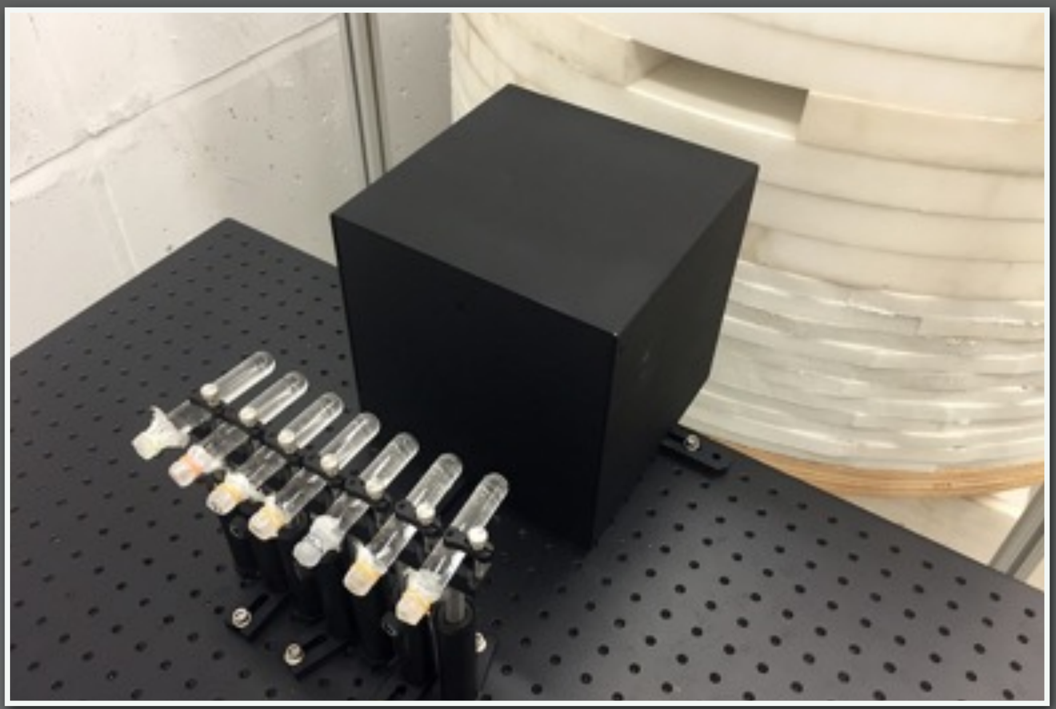
PREVENTING THE EXCHANGE OF SENSITIVE INFORMATION DURING A RADIATION MEASUREMENT

Trusted Information Barrier

Measure (but sanitize) sensitive information

“Hard” to authenticate and certify

Single-bit observation



Interactive Zero-knowledge Proof

Never measure sensitive information

“Easy” to authenticate and certify

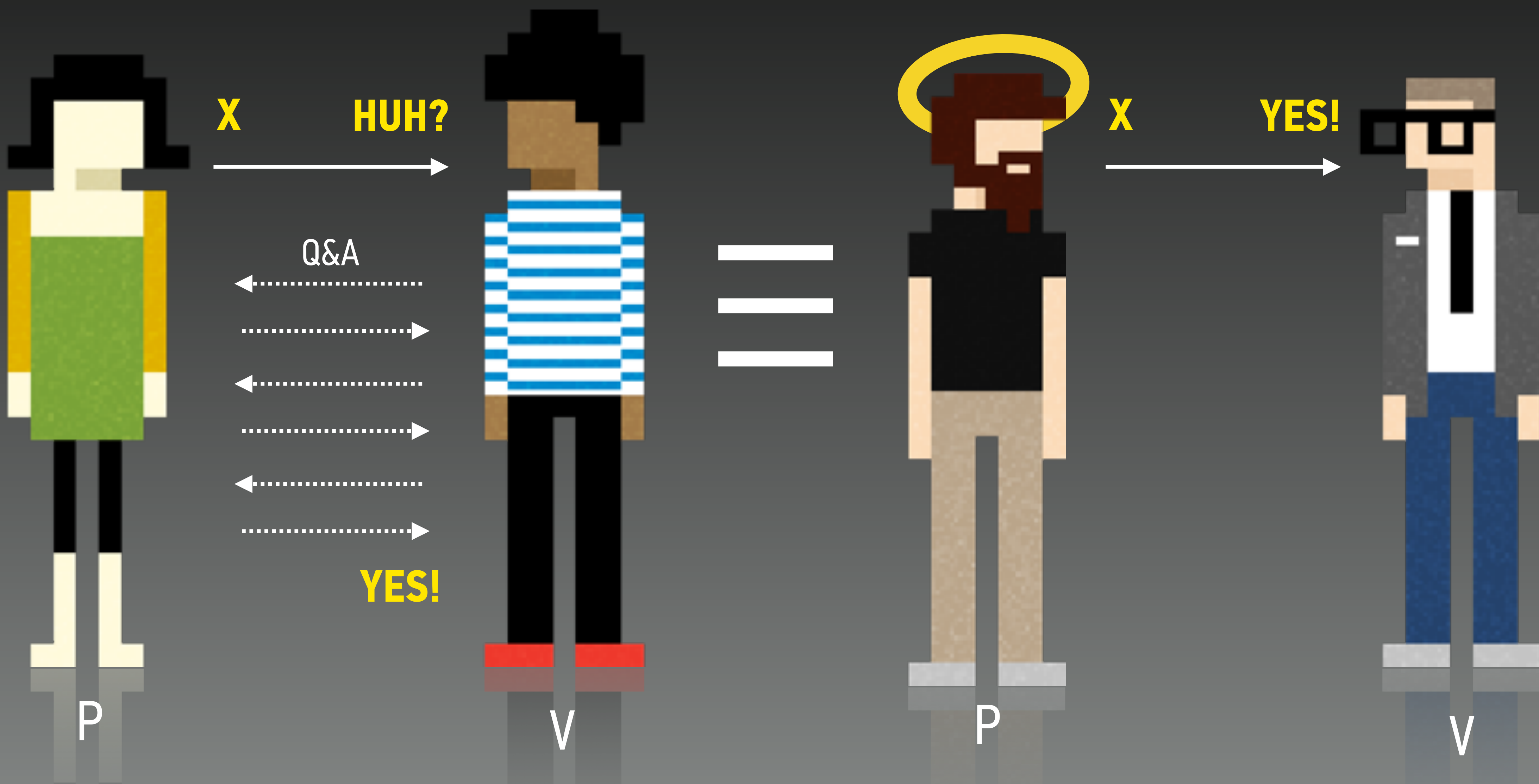
More complex observation

S. Philippe, B. Barak, and A. Glaser, “Designing Protocols for Nuclear Warhead Verification”
56th Annual INMM Meeting, July 12-16, 2015, Indian Wells, California

INTERACTIVE ZERO-KNOWLEDGE PROOFS

LOGICAL LAYER

INTERACTIVE ZERO-KNOWLEDGE 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

EXAMPLE

FOR AN “ILLUSTRATED PRIMER” ON ZERO-KNOWLEDGE PROOFS, SEE
blog.cryptographyengineering.com/2014/11/zero-knowledge-proofs-illustrated-primer.html

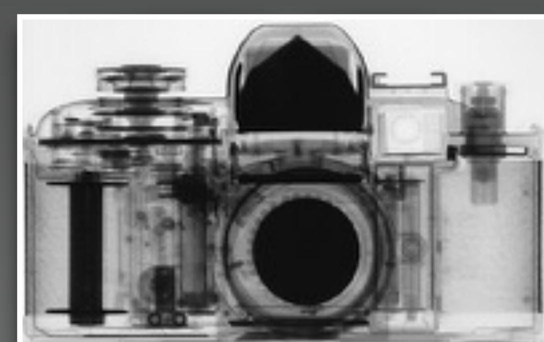
FOR A ZERO-KNOWLEDGE “SUDOKU” PROOF, SEE
www.wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO/

PROVING THAT TWO OBJECTS ARE IDENTICAL

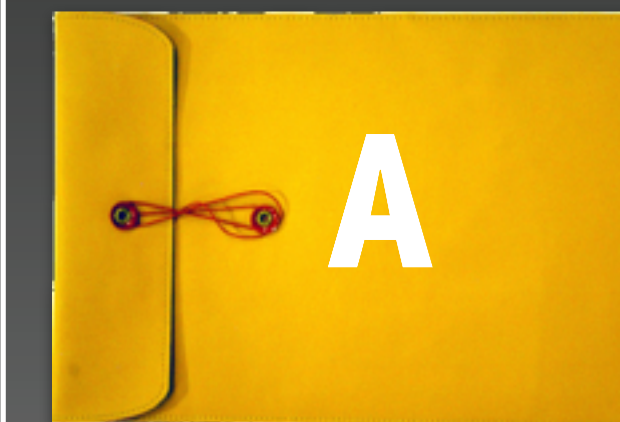
"THE DAY BEFORE THE INSPECTION"

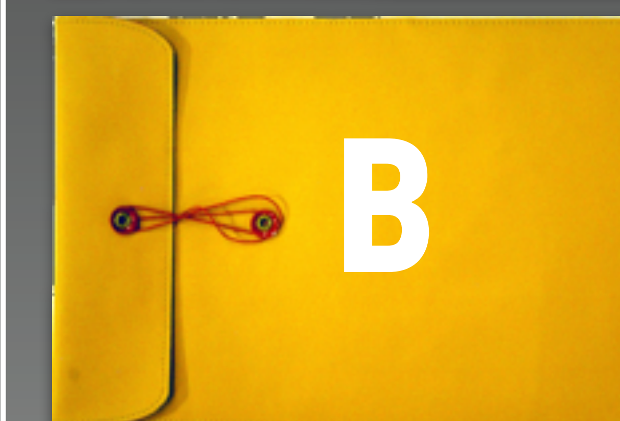
1

2



3





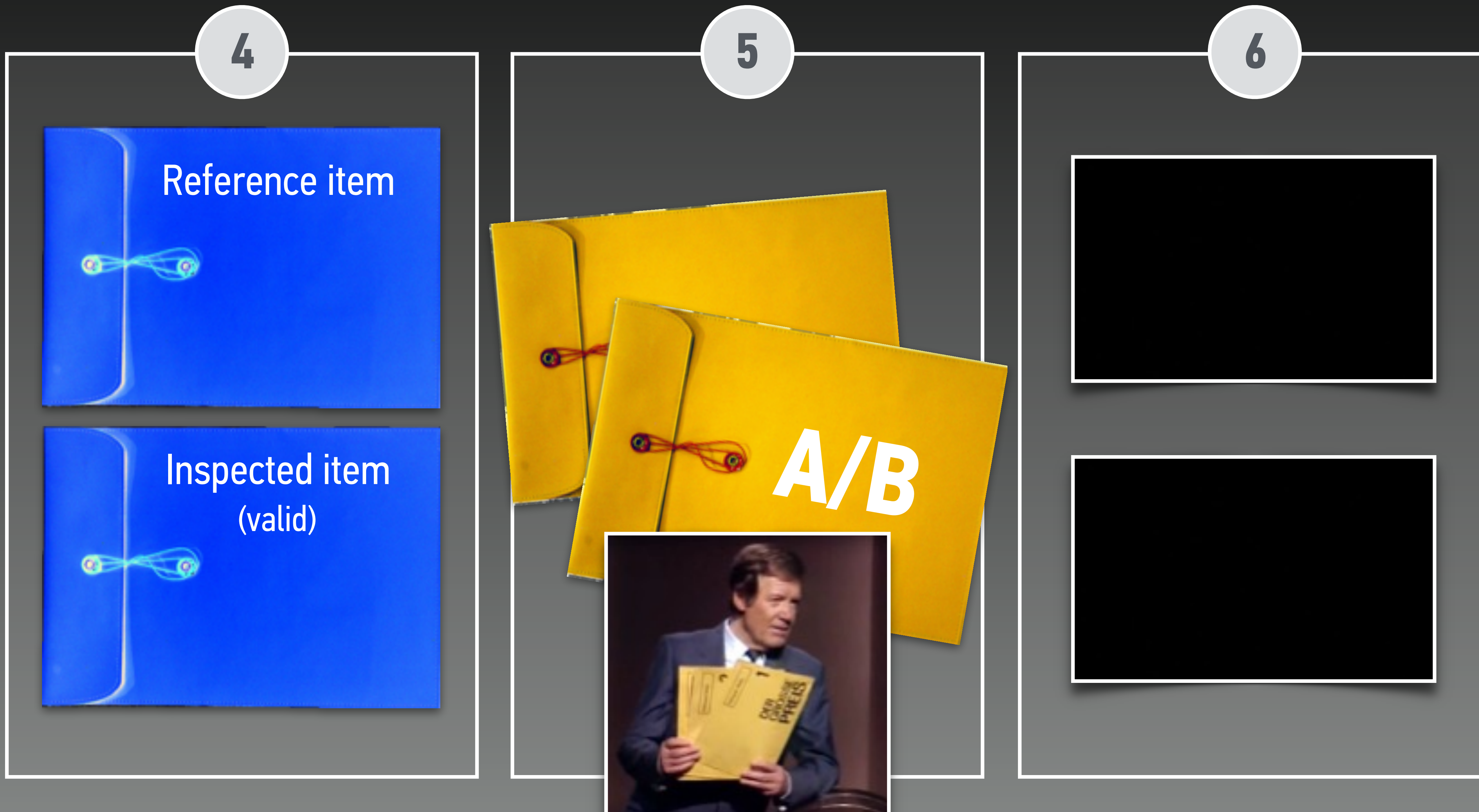
(1) Alice owns valuable objects whose design she wants to keep a secret

(2) In private, she takes a radiograph of this object on "blank film"

(3) Alice prepares two identical complements of that picture and places these complements in two sealed envelopes

PROVING THAT TWO OBJECTS ARE IDENTICAL

"THE DAY OF THE INSPECTION"



(4) At the day of the inspection, Alice presents a reference item and an item for inspection in concealed form

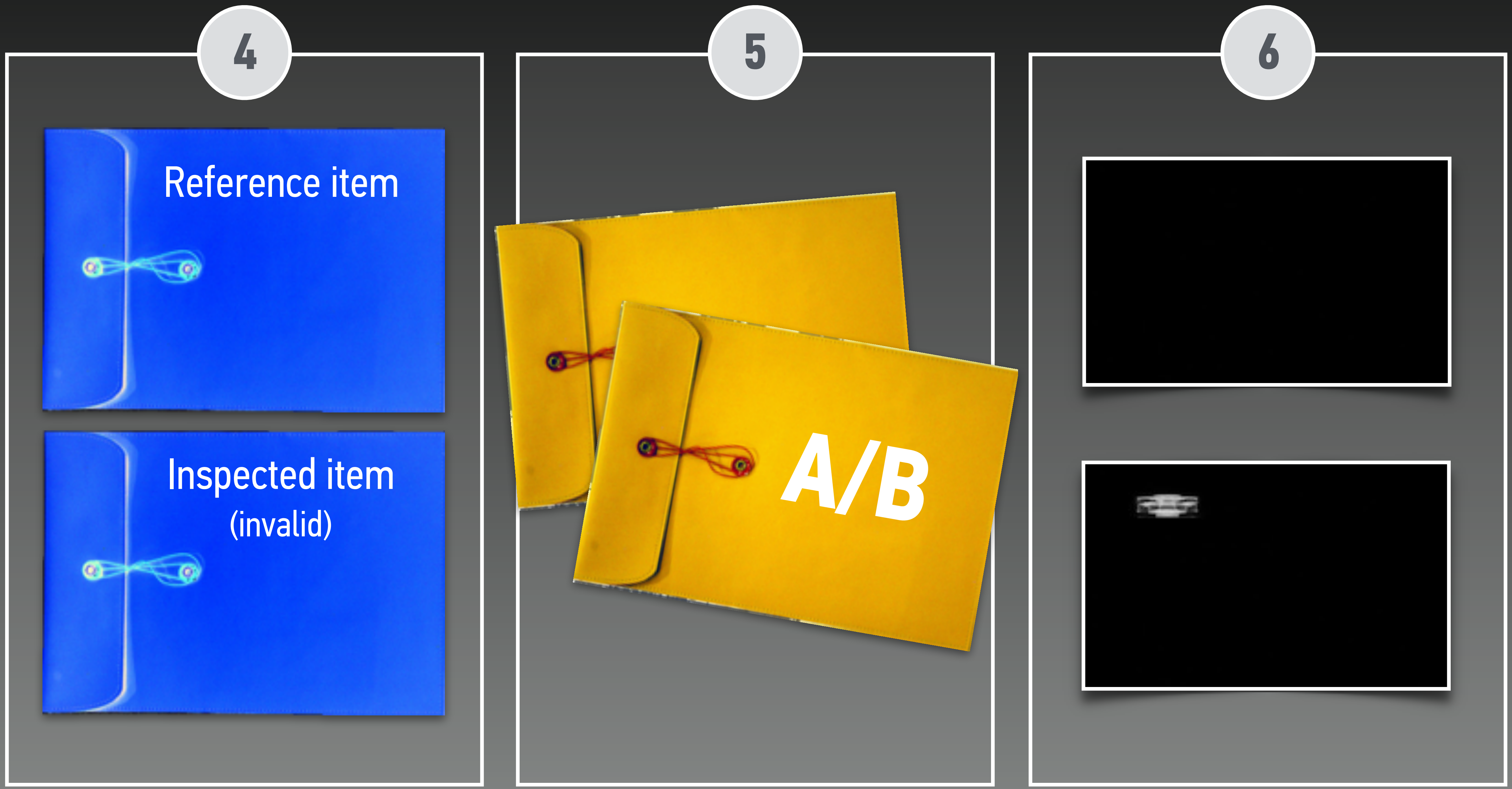
(5) Bob randomly assigns the envelopes; then, new radiographs of both items are made

(6) If Alice presents a valid item, a "flat image" is produced; if not, she risks failing the inspection (and revealing information)

Source: ZDF.de (August 8,1985)

PROVING THAT TWO OBJECTS ARE IDENTICAL

"THE DAY OF THE INSPECTION"



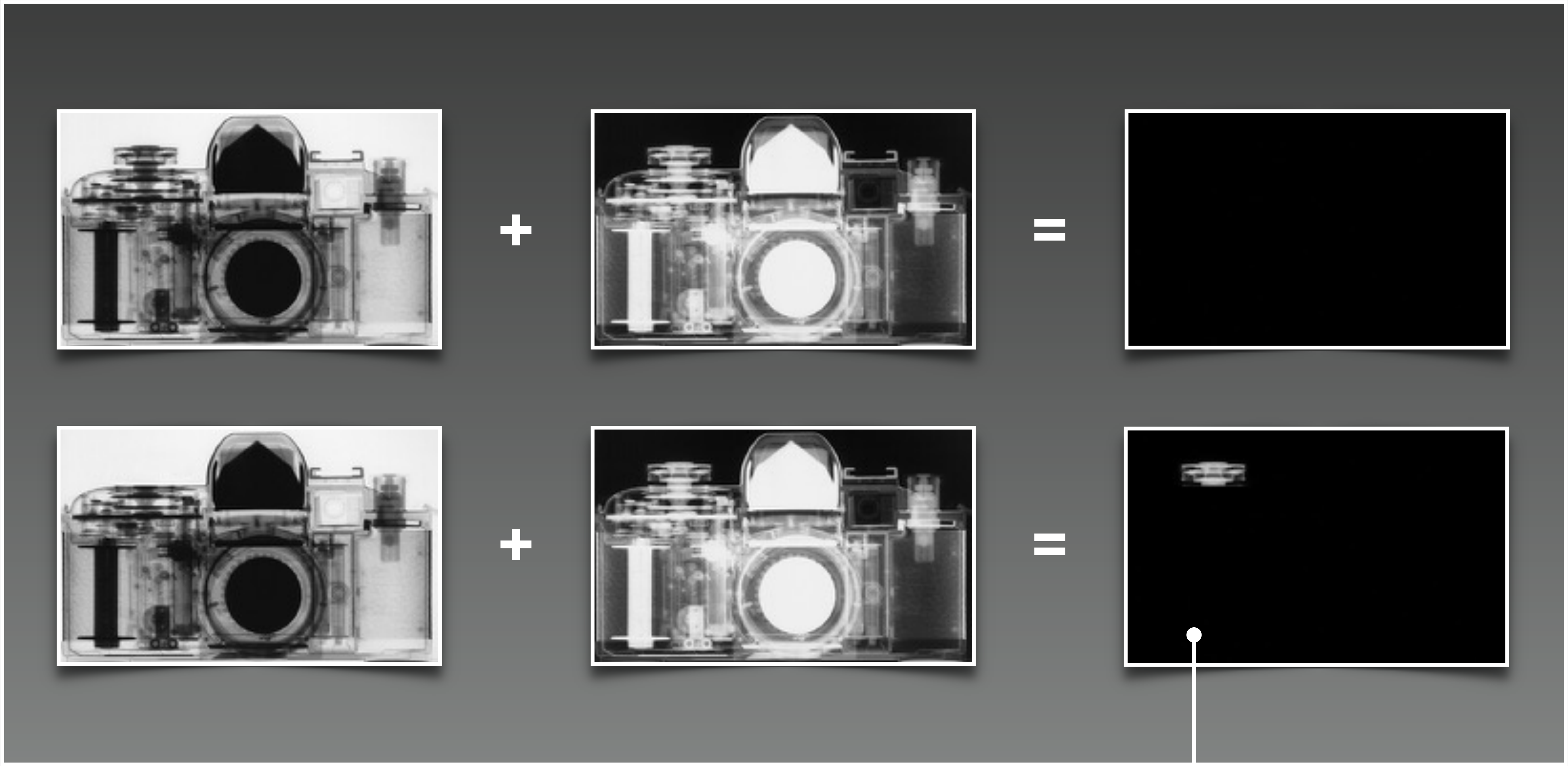
(4) At the day of the inspection, Alice presents a reference item and an item for inspection in concealed form

(5) Bob randomly assigns the envelopes; then, new radiographs of both items are made

(6) If Alice presents a valid item, a "flat image" is produced; if not, she risks failing the inspection (and revealing information)

PROVING THAT TWO OBJECTS ARE IDENTICAL

"THE DAY OF THE INSPECTION"



We will later introduce the maximum possible exposure as "N_{MAX}"

WHAT THE PROTOCOL ACHIEVES

COMPLETENESS

If the items are identical and both host and inspector follow the protocol,
then the inspector will accept with probability $p = 1 - (½)^n$

SOUNDNESS

If the items are different and the inspector follows the protocol,
then, no matter what the host does, the inspector will reject with probability $p \geq 1 - (½)^n$

ZERO KNOWLEDGE

As long as the host follows the protocol and presents matching items,
the inspector gains no knowledge during their interaction except for the fact that the items match

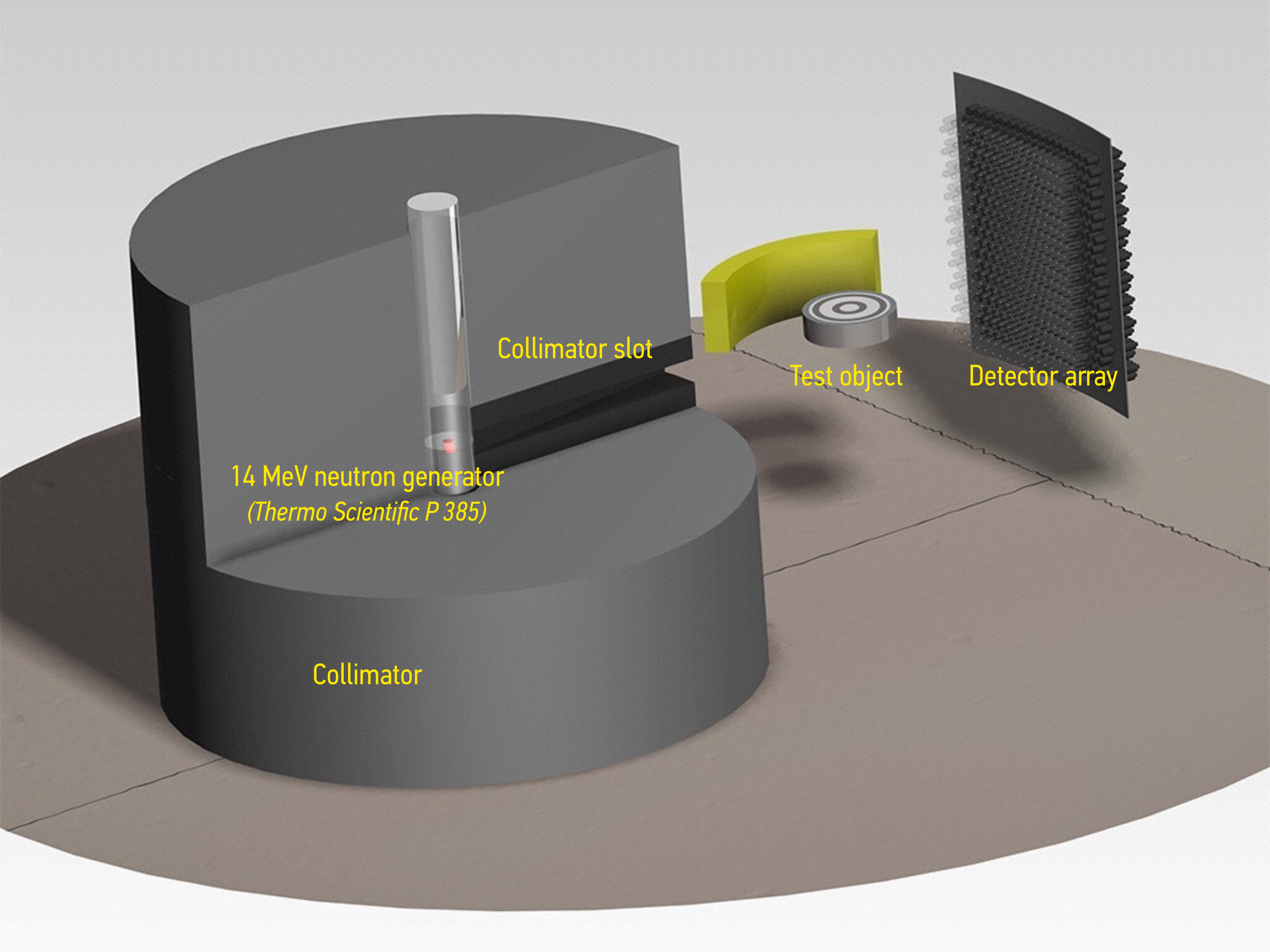
S. Philippe, B. Barak, and A. Glaser, "Designing Protocols for Nuclear Warhead Verification"
56th Annual INMM Meeting, July 12-16, 2015, Indian Wells, California

PHYSICAL ZERO-KNOWLEDGE PROOFS

WITH NON-ELECTRONIC PRELOADABLE DETECTORS

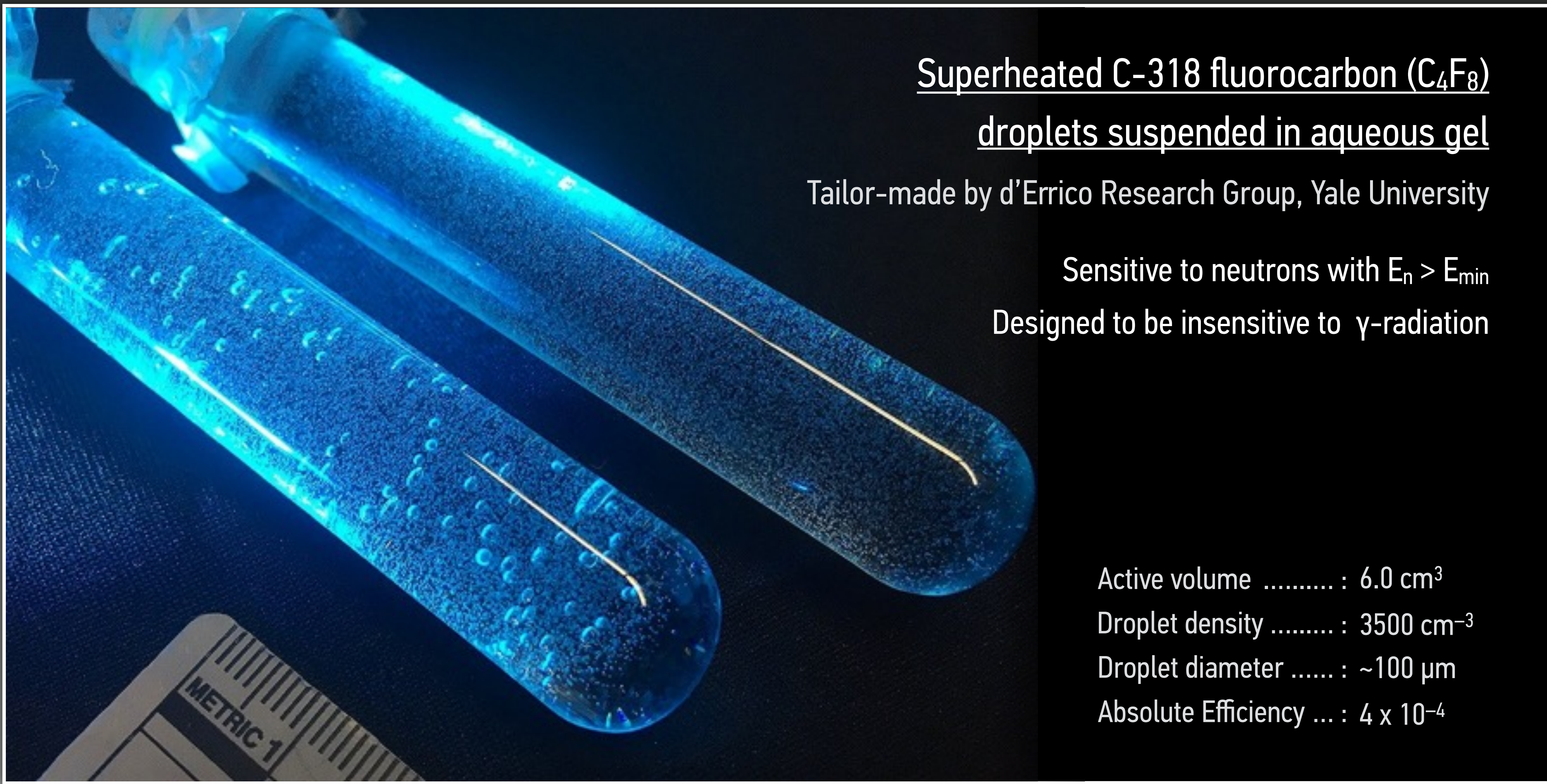
THIS BASIC IDEA HAS TRIGGERED INTEREST IN OTHER “PHYSICAL APPLICATIONS” OF ZERO-KNOWLEDGE

see, for example, B. Fisch, D. Freund, M. Naor, “Physical Zero-Knowledge Proofs of Physical Properties”
Advances in Cryptology, CRYPTO 2014, Lecture Notes in Computer Science, Volume 8617, Springer, Heidelberg, 2014


Collimator slot
Test object
Detector array
14 MeV neutron generator
(Thermo Scientific P 385)
Collimator

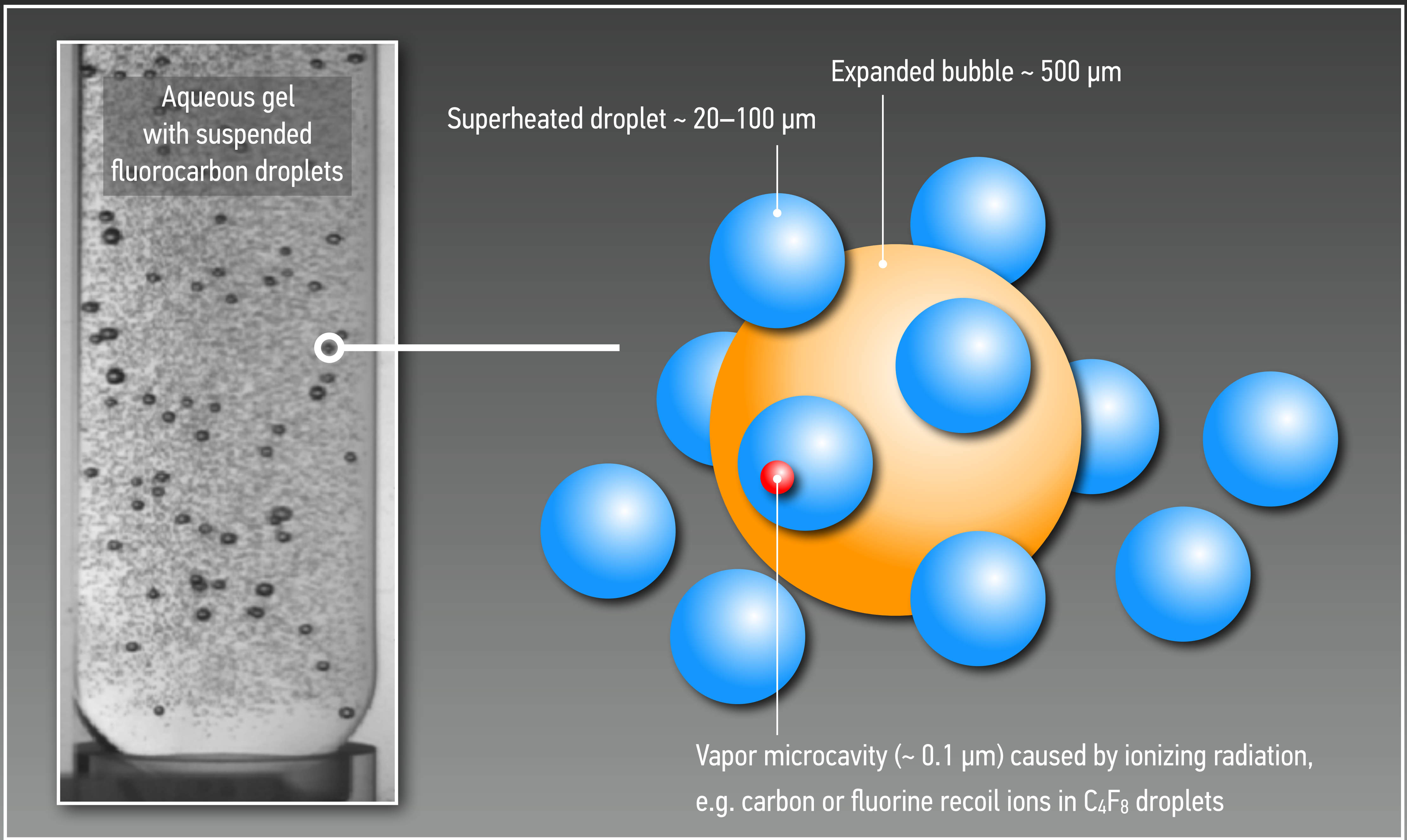
SUPERHEATED DROPLET DETECTORS OFFER A WAY TO IMPLEMENT THIS PROTOCOL

AND AVOID DETECTOR-SIDE ELECTRONICS



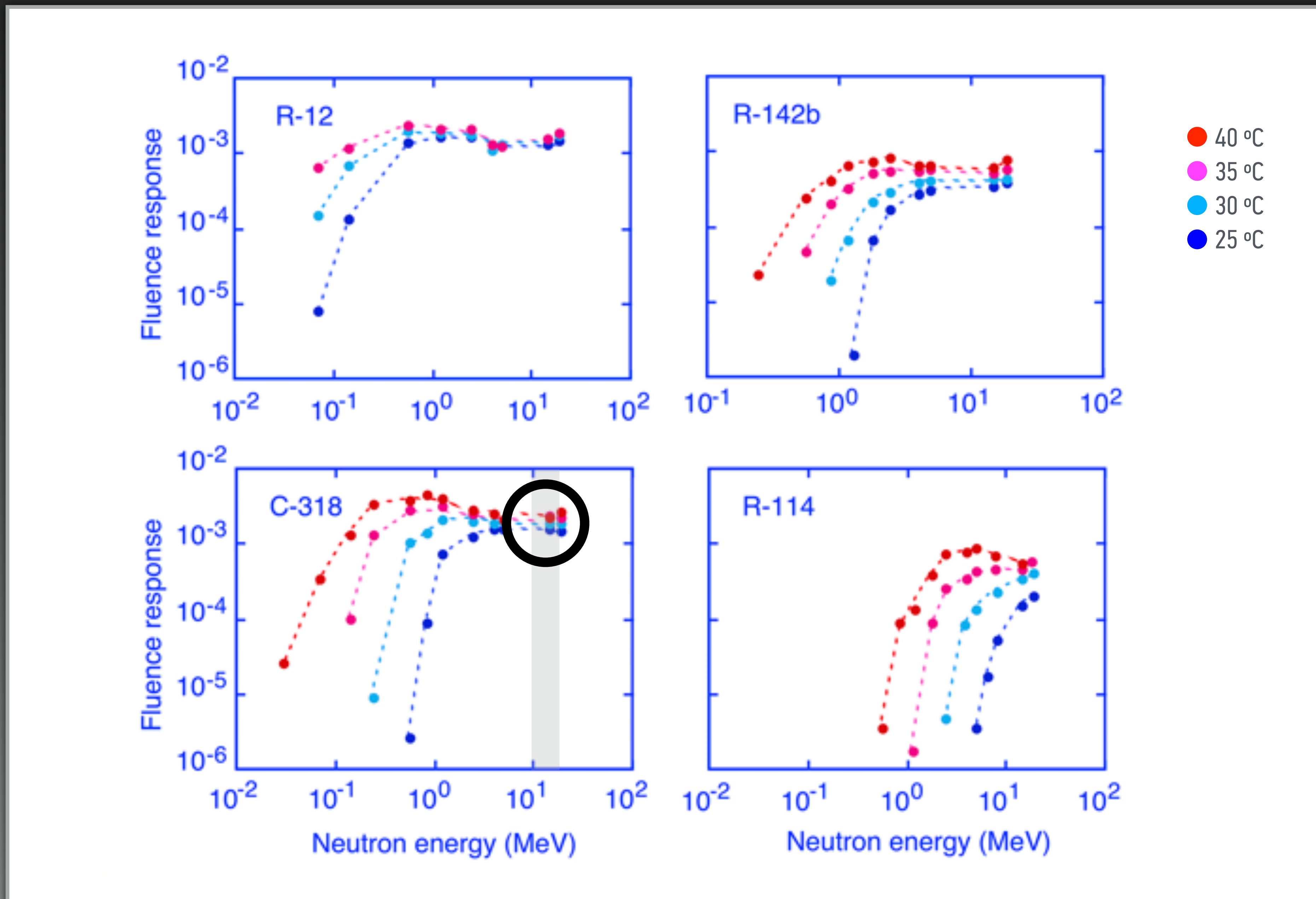
SUPERHEATED DROPLET DETECTORS

PRINCIPLE



FLUENCE RESPONSE

OF SUPERHEATED EMULSIONS MEASURED AS A FUNCTION OF NEUTRON ENERGY AND TEMPERATURE



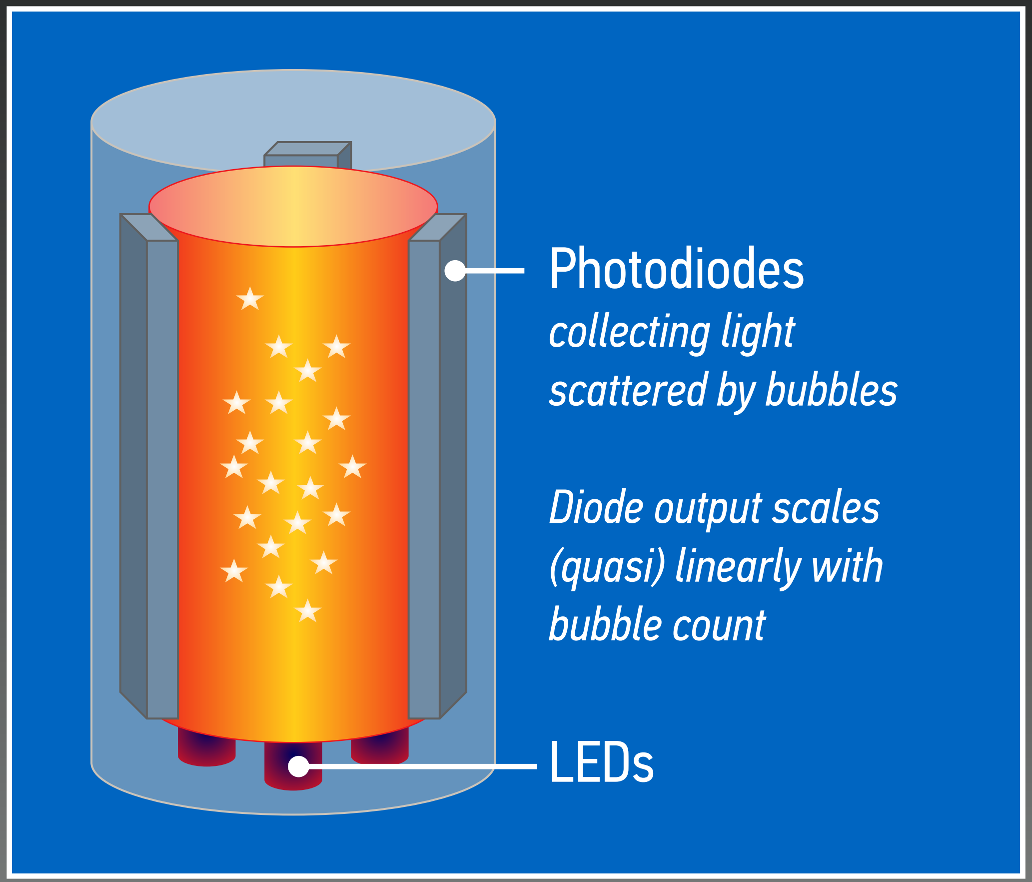
Francesco d'Errico, "Radiation Dosimetry and Spectrometry with Superheated Emulsions"
Nuclear Instruments and Methods in Physics Research B, 184 (2001), pp. 229–254

SUPERHEATED DROPLET DETECTORS

BUBBLES CAN BE COUNTED WITH A VARIETY OF TECHNIQUES

Optical readout (with camera)
Source: Bubble Technologies Industries

Volumetric readout



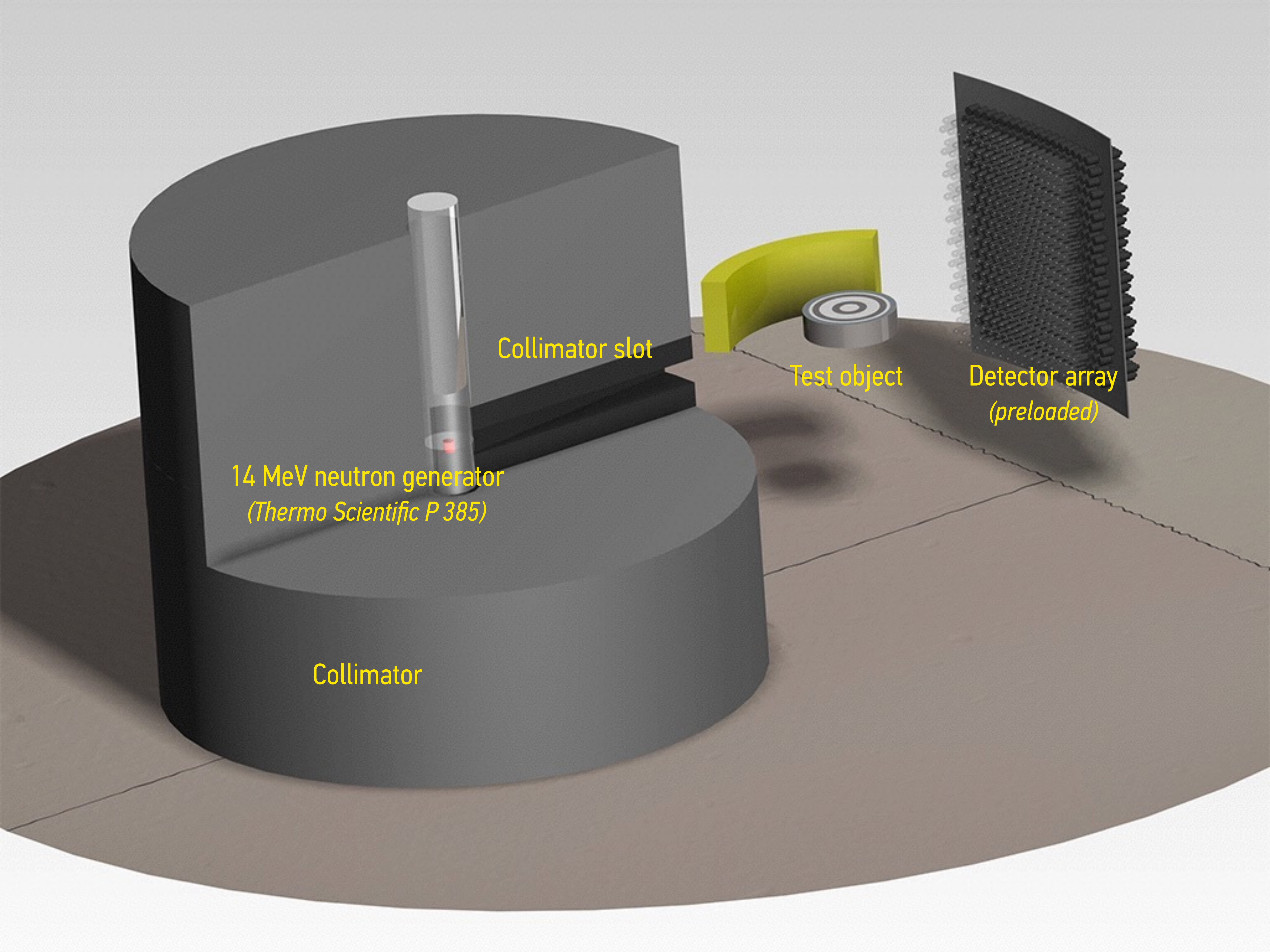
Opto-electronic readout
Adapted from: Francesco d'Errico, Yale

Detectors can be "reset" (bubbles recompressed) many times (good for R&D)

Inspector can verify functionality of detectors after inspection

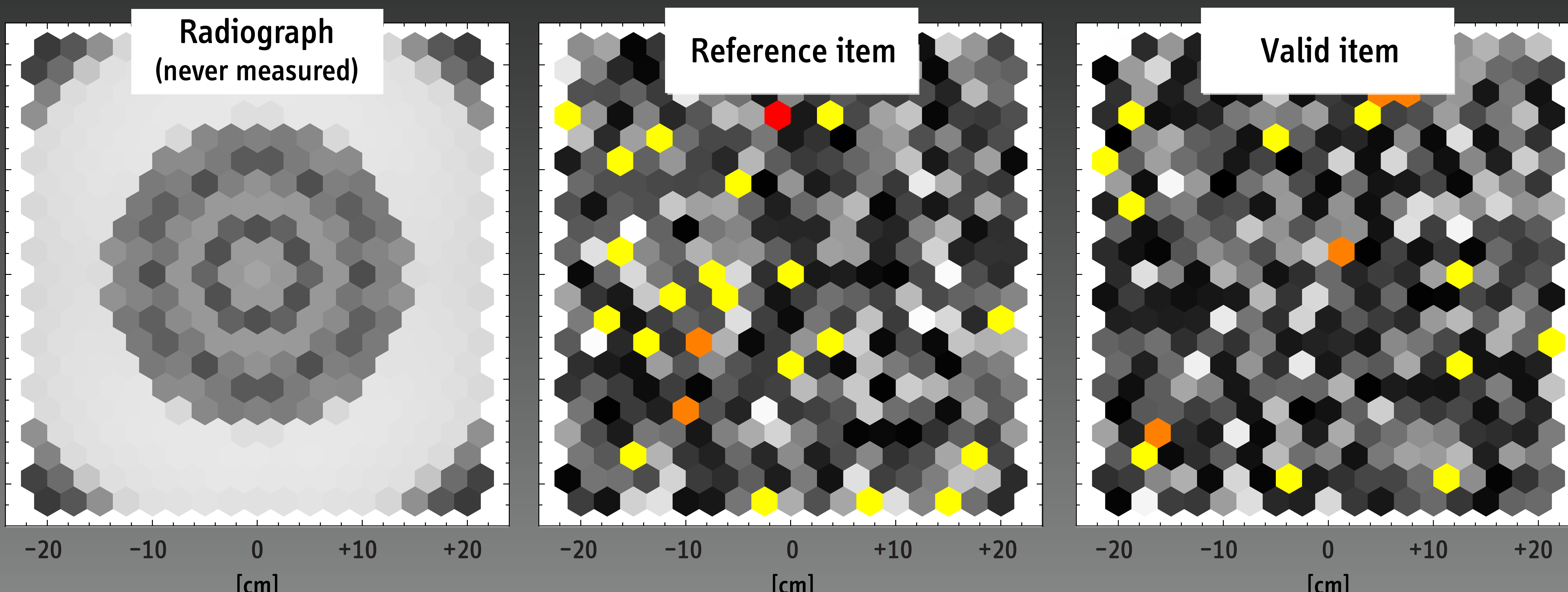
RESULTS

RADIOGRAPHY WITH 14-MeV NEUTRONS
(SIMULATED DATA)


Collimator slot
Test object
Detector array
(preloaded)
14 MeV neutron generator
(Thermo Scientific P 385)
Collimator

ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS



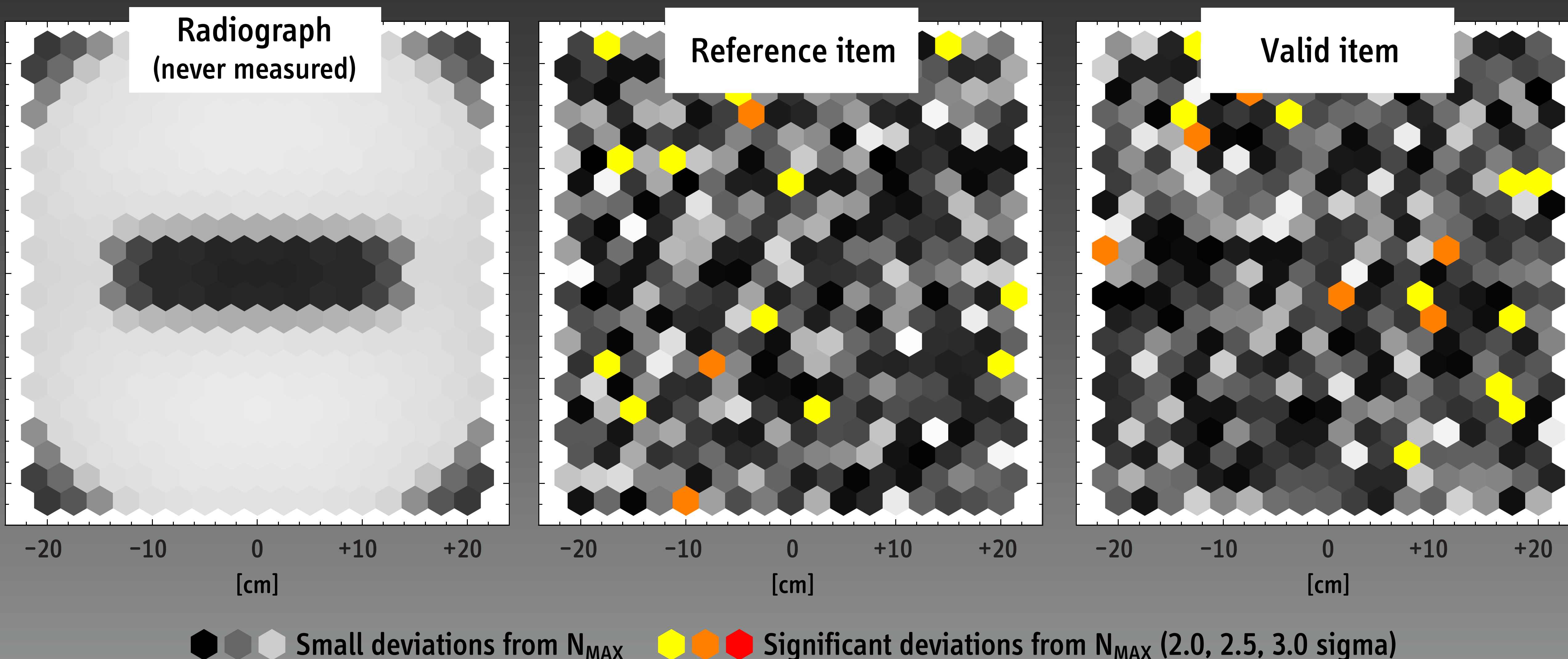
Small deviations from N_{MAX} Significant deviations from N_{MAX} (2.0, 2.5, 3.0 sigma)

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



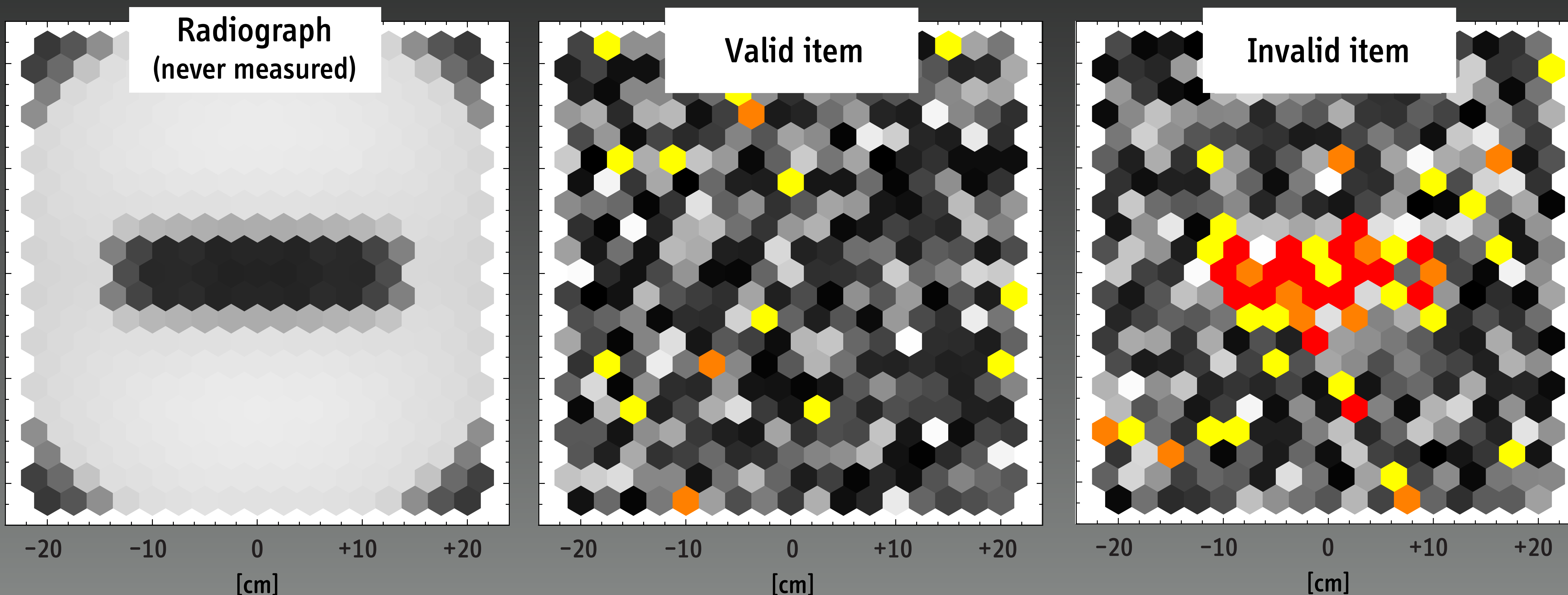
Simulated data from MCNP calculations; neutron detection energies > 10 MeV; N(max) = 5,000

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)



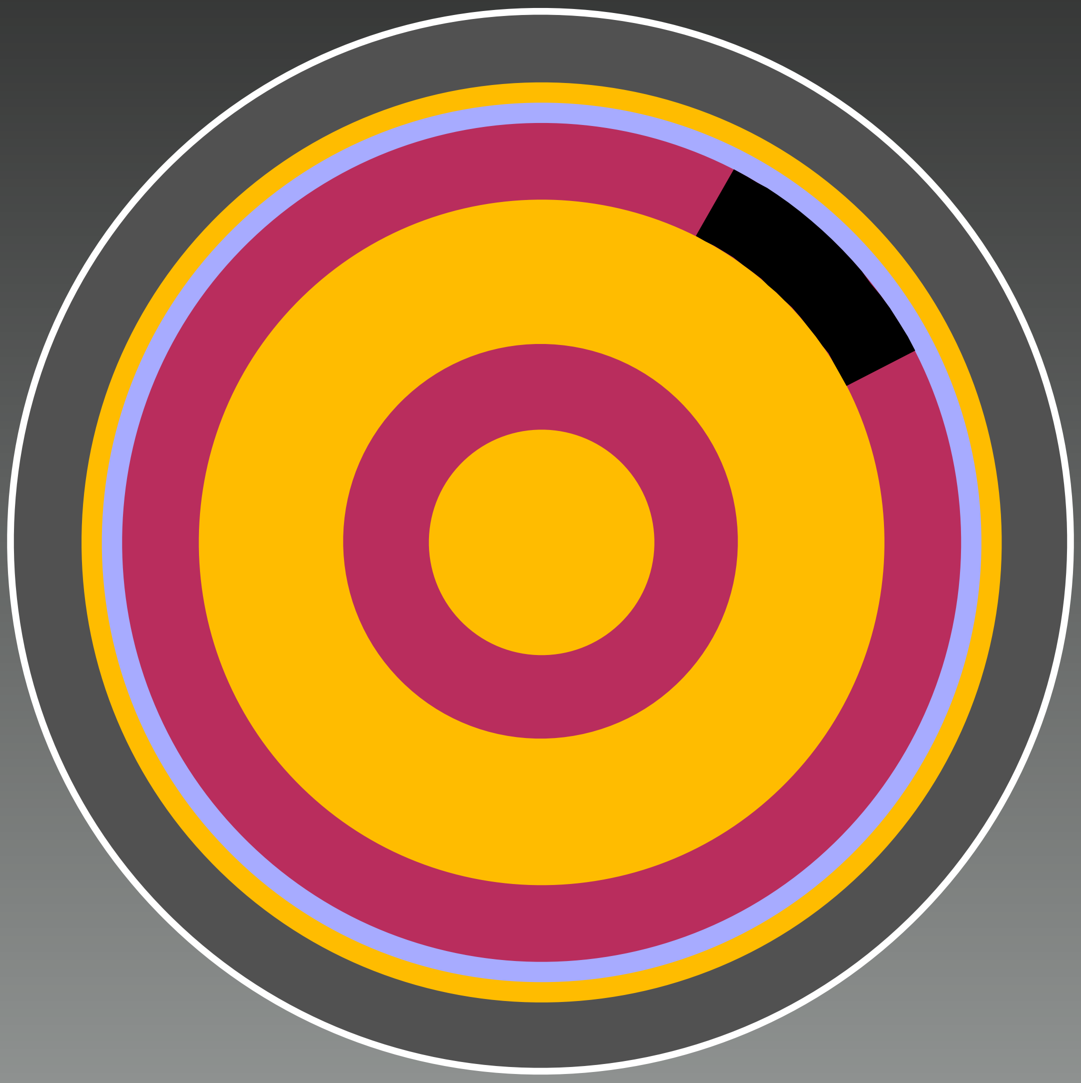
Small deviations from N_{MAX} Significant deviations from N_{MAX} (2.0, 2.5, 3.0 sigma)

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

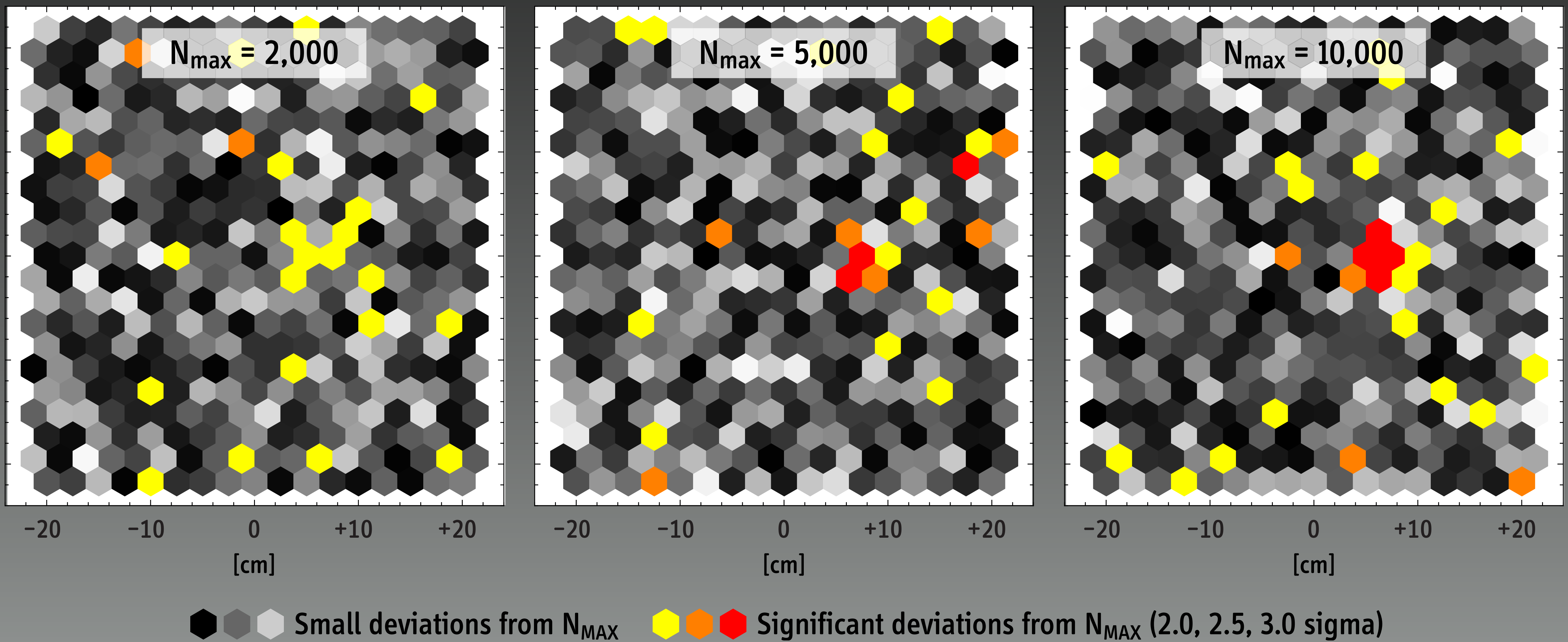
LOCAL TUNGSTEN DIVERSION

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



ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS



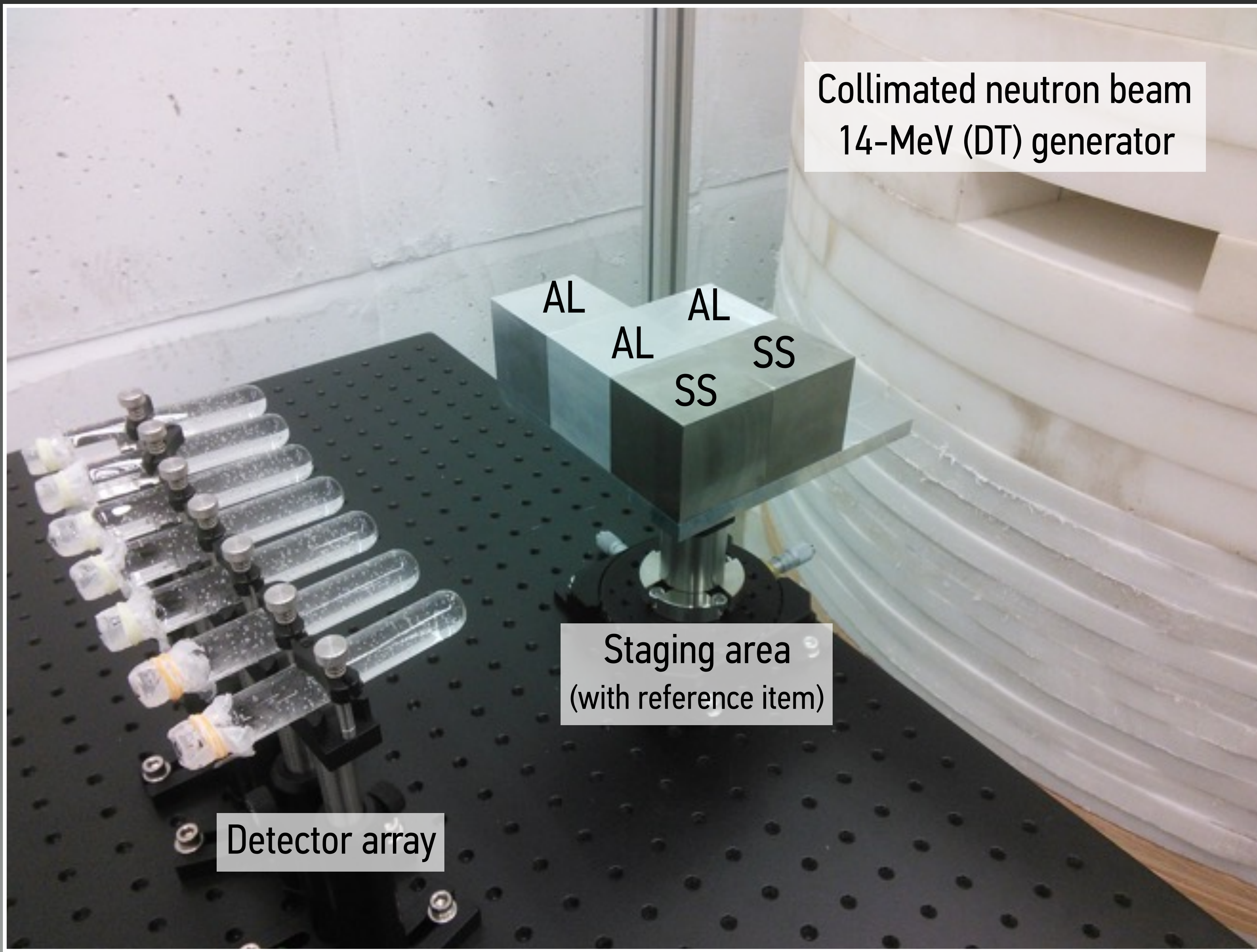
543 grams of tungsten removed from outer ring of test object; simulated data from MCNP calculations; neutron detection energies > 10 MeV
A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502

FIRST EXPERIMENTAL RESULTS

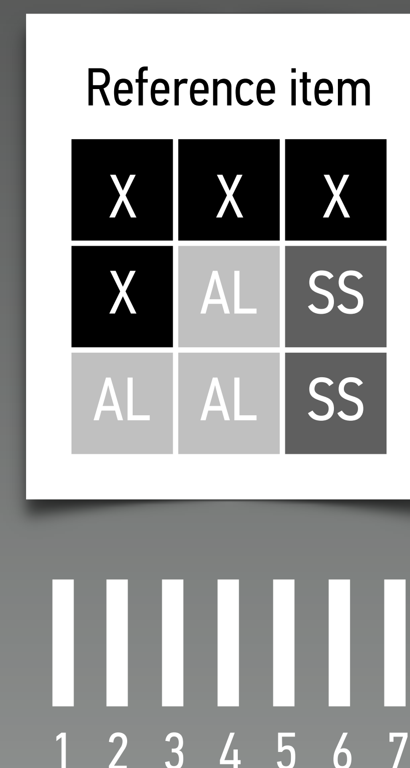
The Conjurer, Hieronymus Bosch, 1502

EXPERIMENTAL SETUP AND SCENARIO

WE WISH TO IDENTIFY CASES IN WHICH THE CUBE PATTERN HAS BEEN ALTERED
WITHOUT GAINING ANY INFORMATION ABOUT THE CONFIGURATION IN CASES WHERE IT HAS NOT



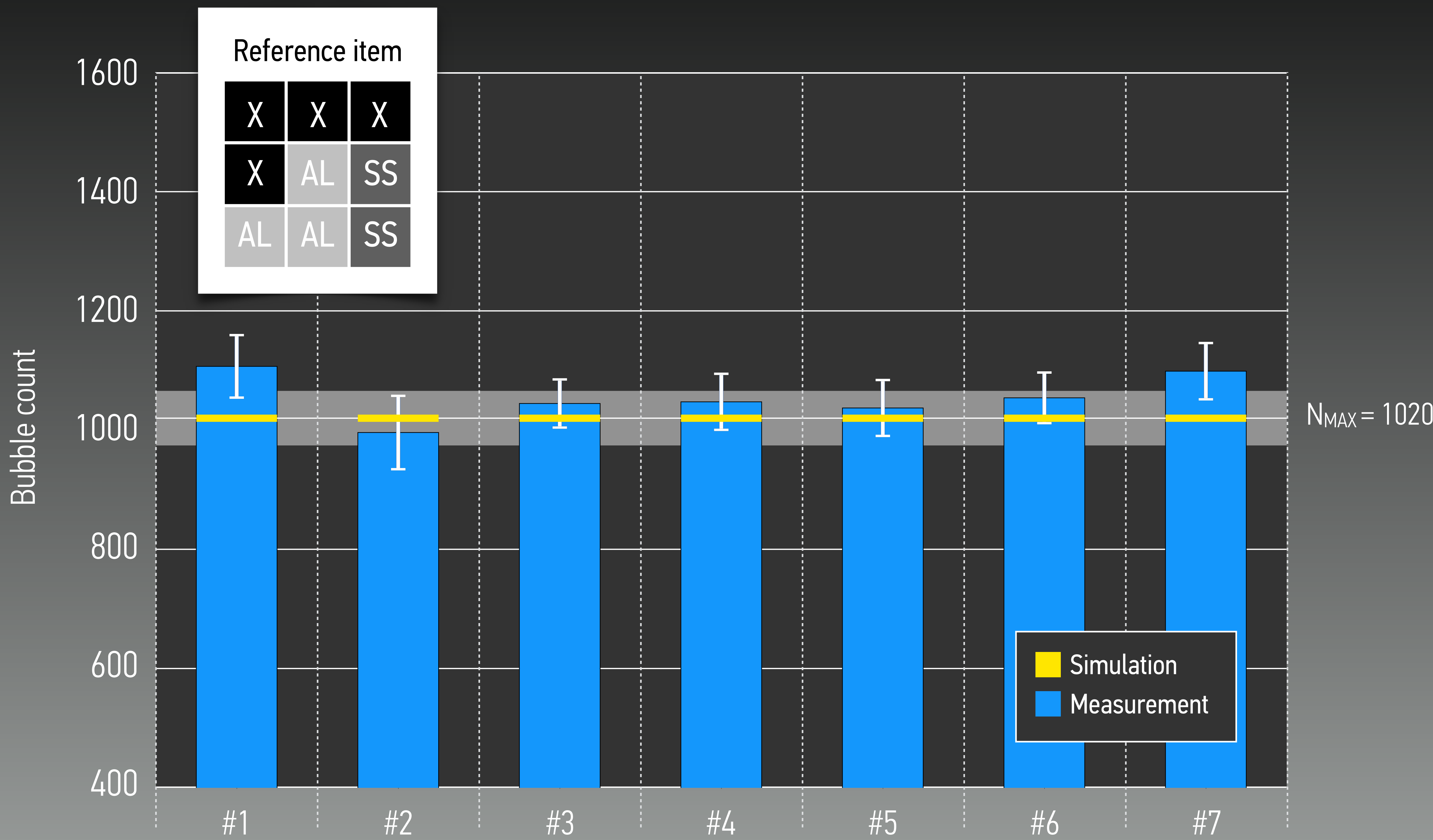
Reference item consists
of a combination of 2-inch cubes
(aluminum and stainless steel)



Detector positions

EXPERIMENTAL RESULTS

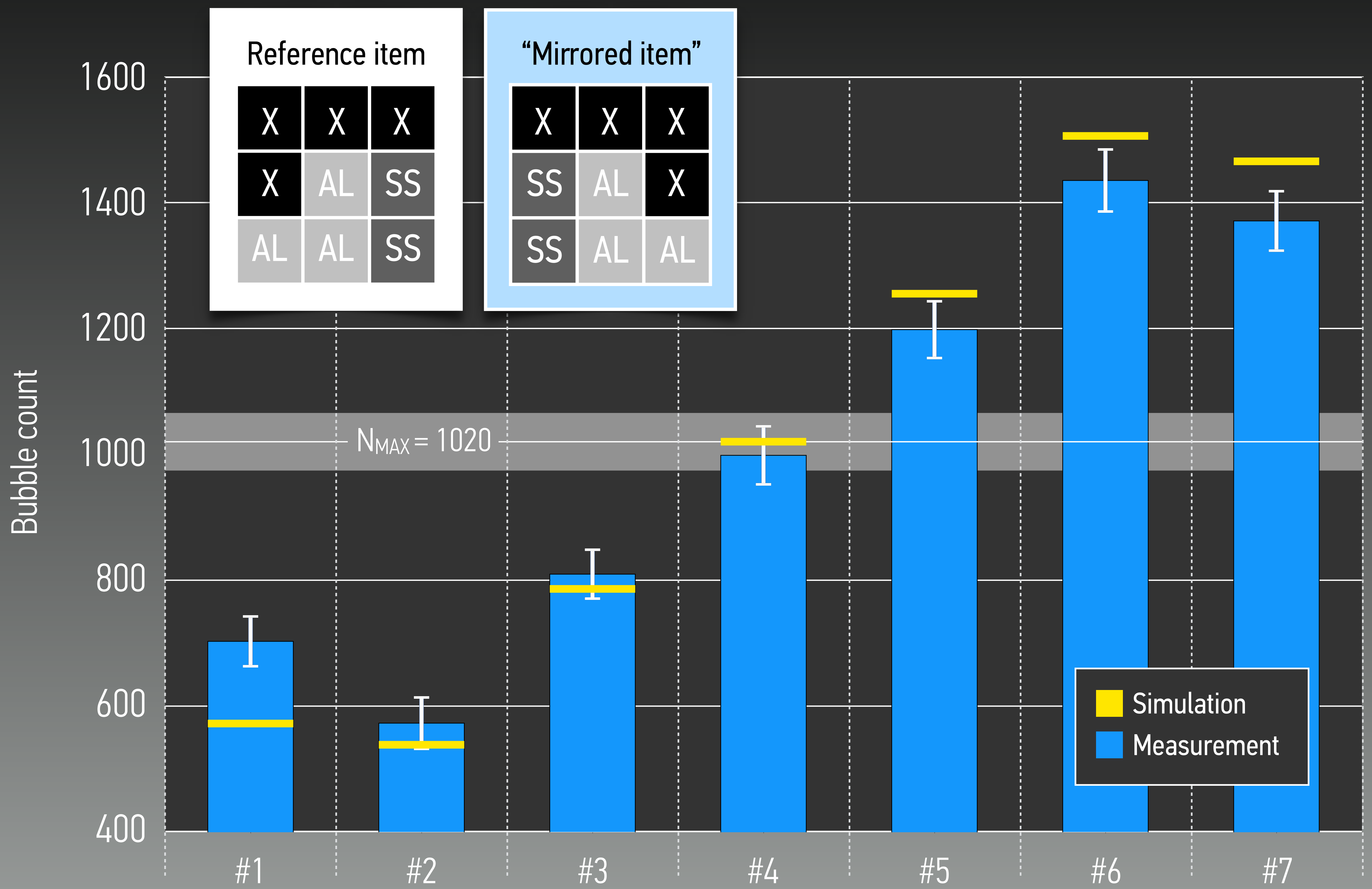
(VALID ITEM)



S. Philippe, R. J. Goldston, A. Glaser and F. d'Errico, "Experimental Demonstration of a Physical Zero-knowledge Protocol for Nuclear Warhead Verification," *under review*

EXPERIMENTAL RESULTS

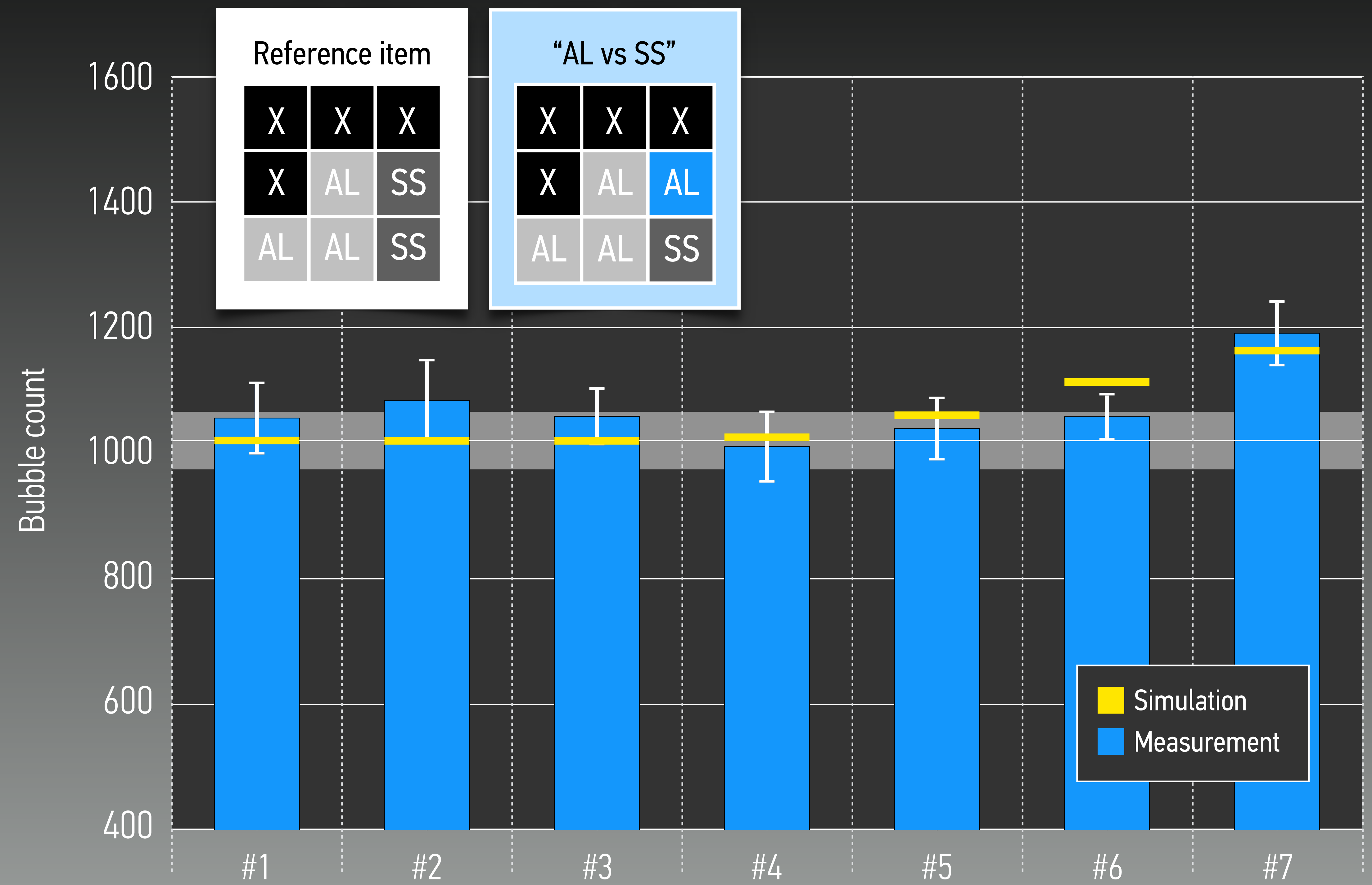
(A DRASTIC CHANGE)



S. Philippe, R. J. Goldston, A. Glaser and F. d'Errico, "Experimental Demonstration of a Physical Zero-knowledge Protocol for Nuclear Warhead Verification," *under review*

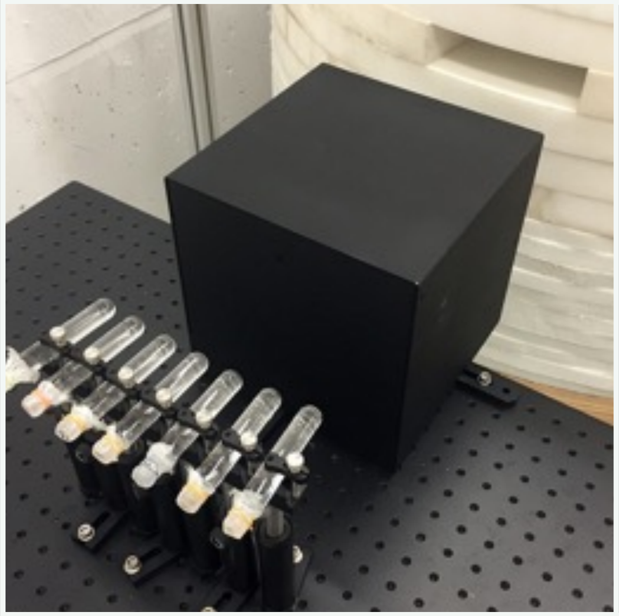
EXPERIMENTAL RESULTS

(A SMALLER CHANGE)



S. Philippe, R. J. Goldston, A. Glaser and F. d'Errico, "Experimental Demonstration of a Physical Zero-knowledge Protocol for Nuclear Warhead Verification," *under review*

NEXT STEPS / WAY FORWARD



AT LAB-SCALE: DEMONSTRATING ZERO-KNOWLEDGE APPROACHES

- Experimental reproducibility of results
- Maximize bubble loading (and confirm absence of bubble “aging”)
- Two-color setting (e.g. 300 keV and 14 MeV neutrons)
- Data commitment schemes

BEYOND LAB-SCALE: TOWARD FULL-SCALE INSPECTION SYSTEMS

- Experiments with special nuclear materials in real-world conditions
  Measurements at the Nevada National Security Site planned for … next week
- Leveraging the virtues of unclassified research
  Multidisciplinary, open for blue-sky ideas, involving international partners

Source: U.S. Department of Energy (bottom)

Photo: Mikhail Klimentyev/AP

ACKNOWLEDGEMENTS

PRINCETON AND PPPL

Andrew Carpe
Charles Gentile
Robert J. Goldston
Sébastien Philippe
Yan Jie

Michael Schöppner
Mark Walker
Bernadette Cogswell
Julien de Troullioud de Lanversin
Tamara Patton

M. V. Ramana
Zia Mian
Frank von Hippel
Malte Göttsche
Benjamin Reimold

ELSEWHERE

Boaz Barak, Microsoft Research New England / Harvard University
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

PRINCETON UNIVERSITY | NUCLEAR FUTURES | LAB