SAND2017-5447C

Office of Defense Nuclear Nonproliferation Research and Development

University Program Review (UPR) 2017 Meeting

Practical Implementation of a Zero Knowledge Protocol for Warhead Verification

NSSC – Nuclear Science & Security Consortium

June 6, 2017

Rebecca Krentz-Wee
UC-Berkeley

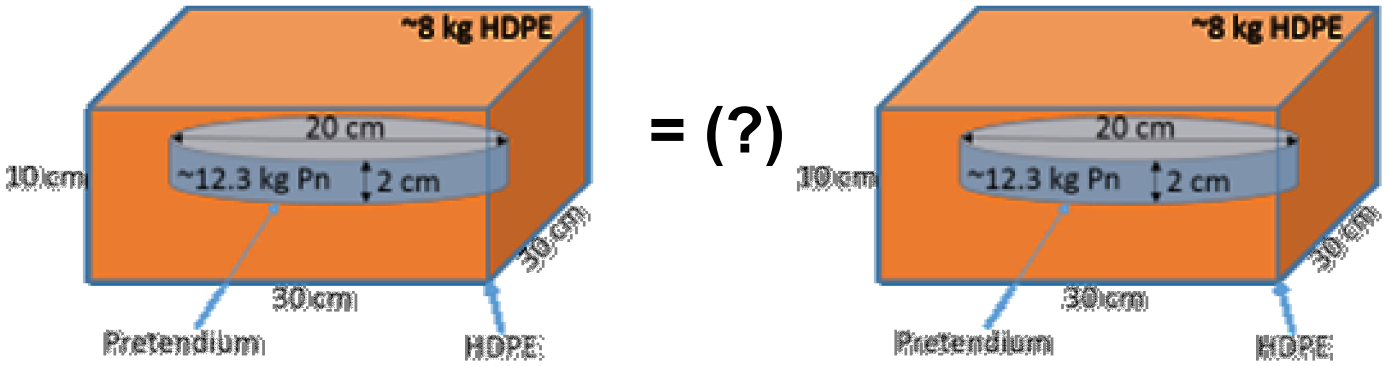
Implementation of a Zero Knowledge Protocol for Warhead Verification

- **Project: CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding (CONFIDANTE)**
- **Goal: Implement and characterize a ZKP for warhead verification**
- **Peter Marleau, Sandia National Labs**
- **Rebecca Krentz-Wee, UC-Berkeley, NSSC**
- **Patricia Schuster, University of Michigan, CVT affiliate**

Challenge: Item Authentication & Certification

Authentication - the process by which a monitoring party gains confidence that reported characteristics of an entity reflect the true state of that entity

Certification – the process by which a host party gains confidence that sensitive information regarding an entity or facility remains secure.

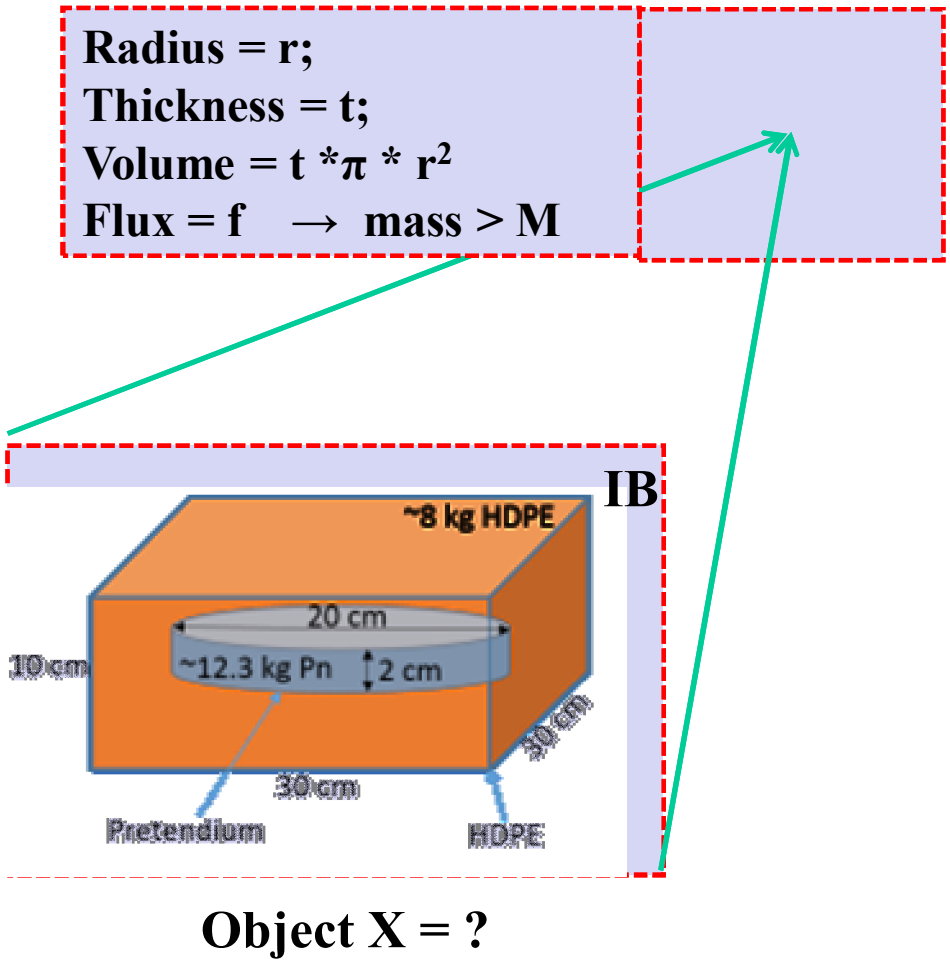


Object T = valid type 1 TAI

Object X = ?

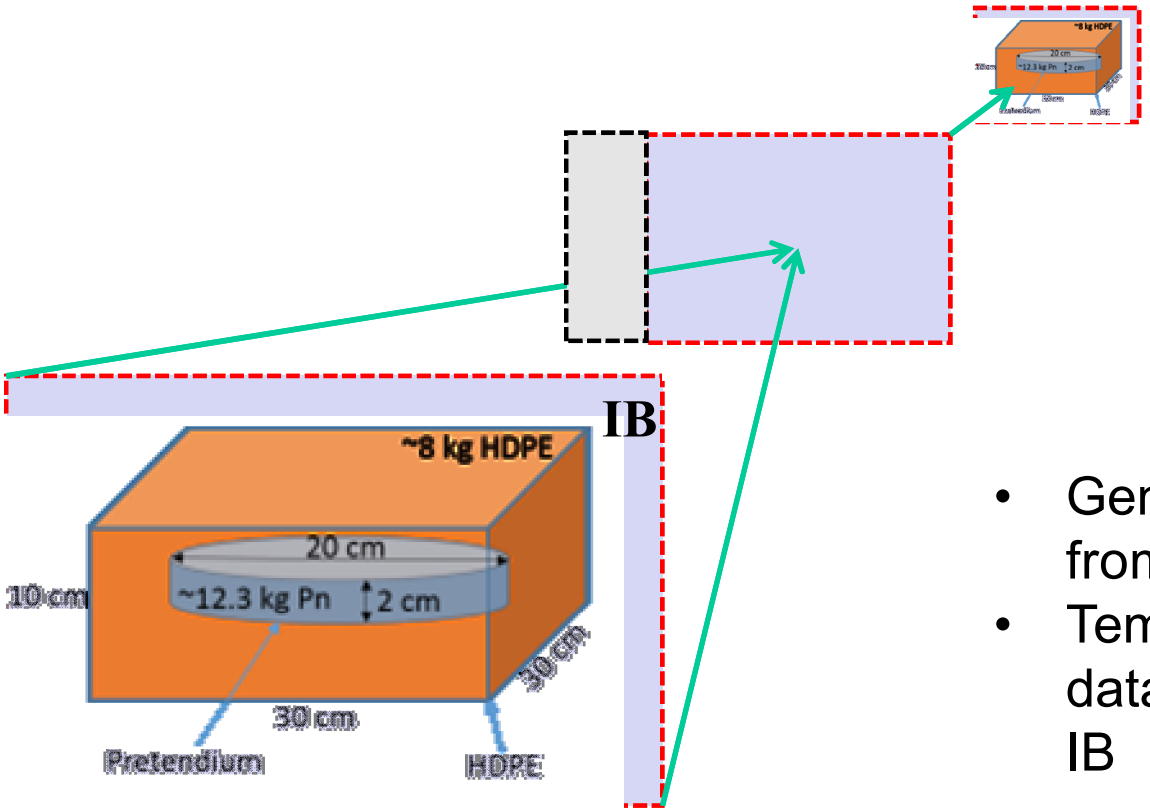
E. Brubaker, "Workshop on Techniques for Protection of Imaging Information: Challenge Problem", SAND2016-4047 O

Current Verification Methods: Attribute



- Define relevant & specific attributes
- Derive attributes from measurements
- Compare with acceptable threshold values
- Measurement and values all sensitive information

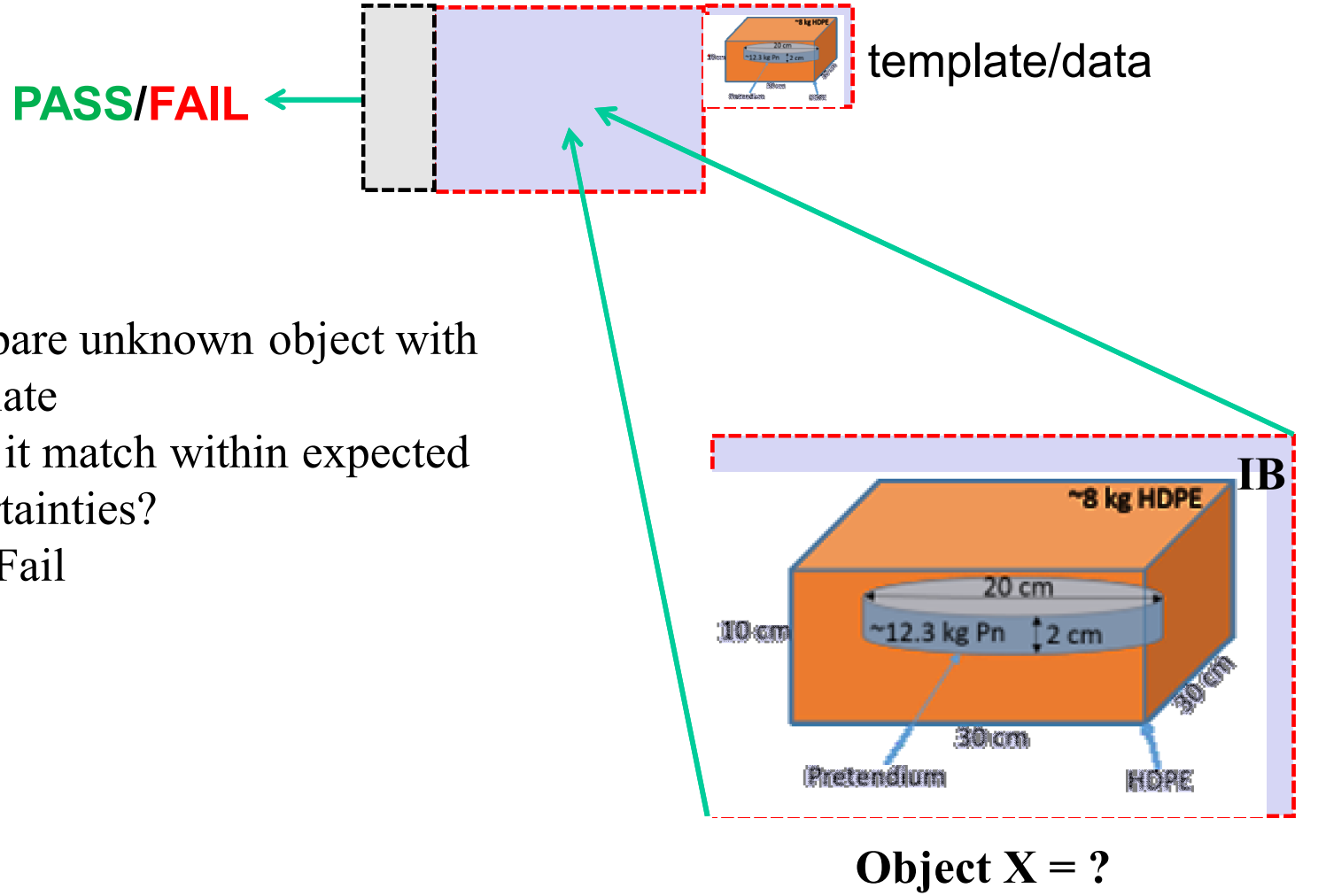
Current Verification Methods: Template



Object T = valid type
1 TAI

- Generate a template from a verified object
- Template has sensitive data, so stored behind IB

Current Verification Methods: Template



- Compare unknown object with template
- Does it match within expected uncertainties?
- Pass/Fail

Two Current Verification Methods

Attribute

- Define relevant & specific attributes
- Derive attributes from measurements
- Compare with acceptable threshold values
- **Measurement and values behind IB**

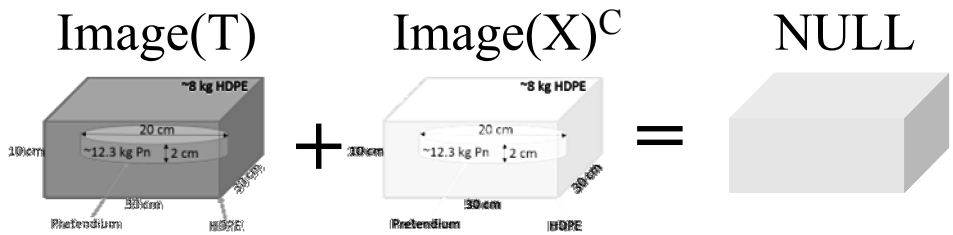
Template

- Generate template from verified object
- Compare unknown object with template
- **Template (device and measurement) behind IB**

Only the final Pass/Fail can be seen by both parties.

Can we decrease the amount of information behind a barrier while still maintaining confidence?

ZKP: Complementary Comparison

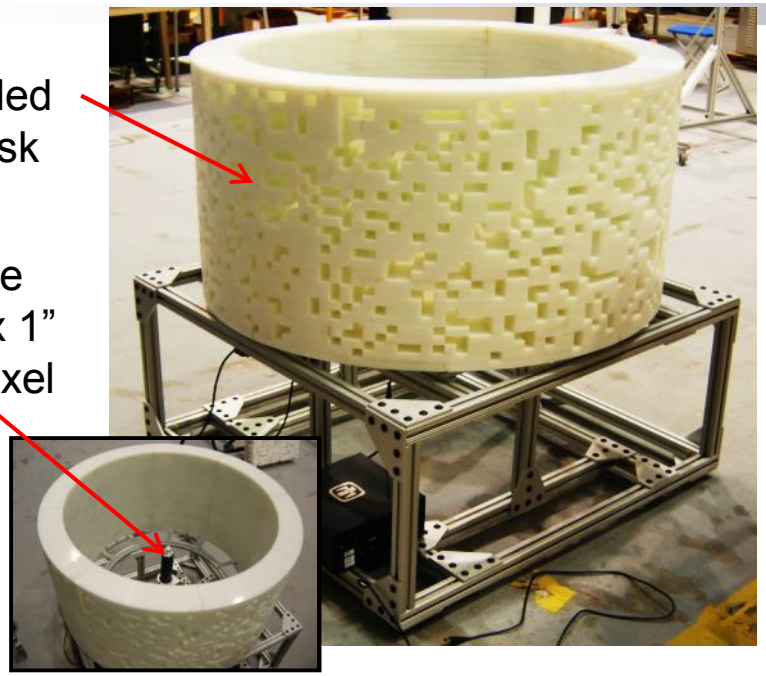


- An image added to its complement produces a null result
- Null result
  - Confirms two original objects are the same
  - Contains zero sensitive information
  - Both parties can view the result
- Is there a way to get a physical NULL as an indication of positive confirmation at all times?

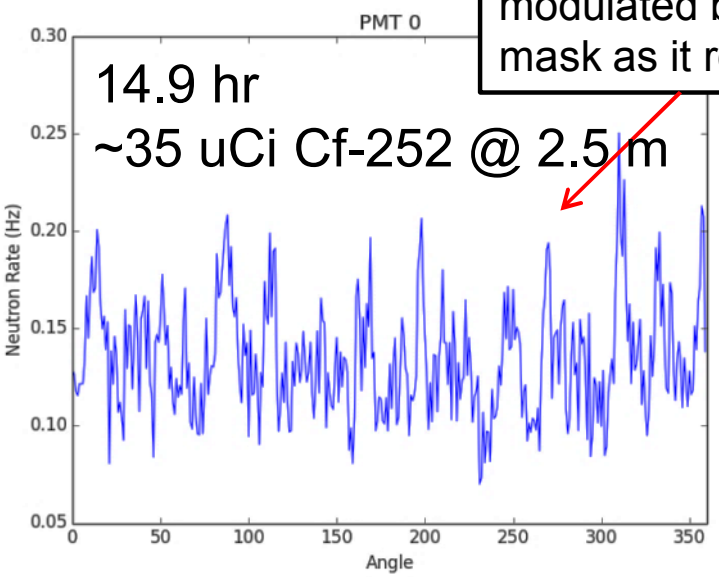
2D Time-Encoded Imaging (TEI)

2-d coded mask

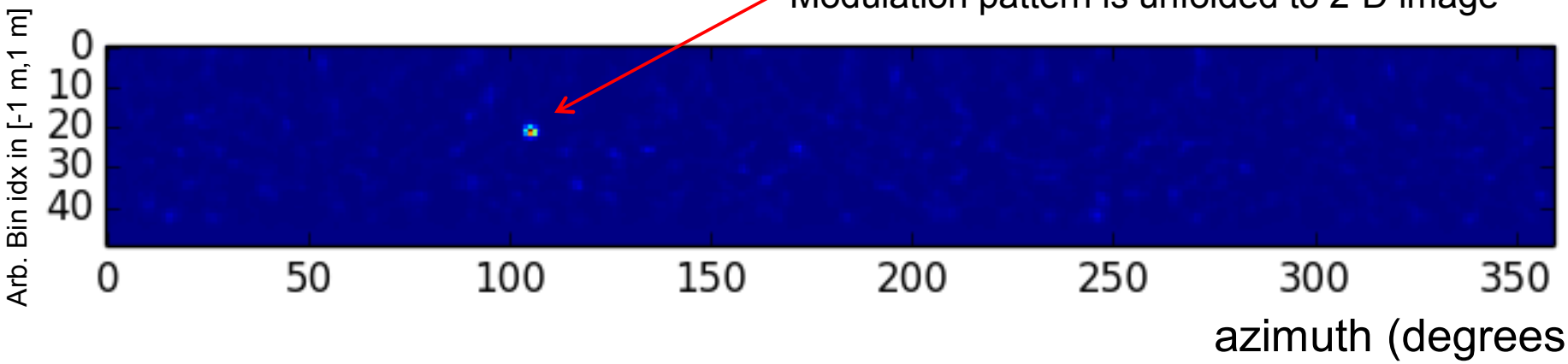
Single 1”D x 1” LS pixel



Single pixel rate is modulated by the mask as it rotates.



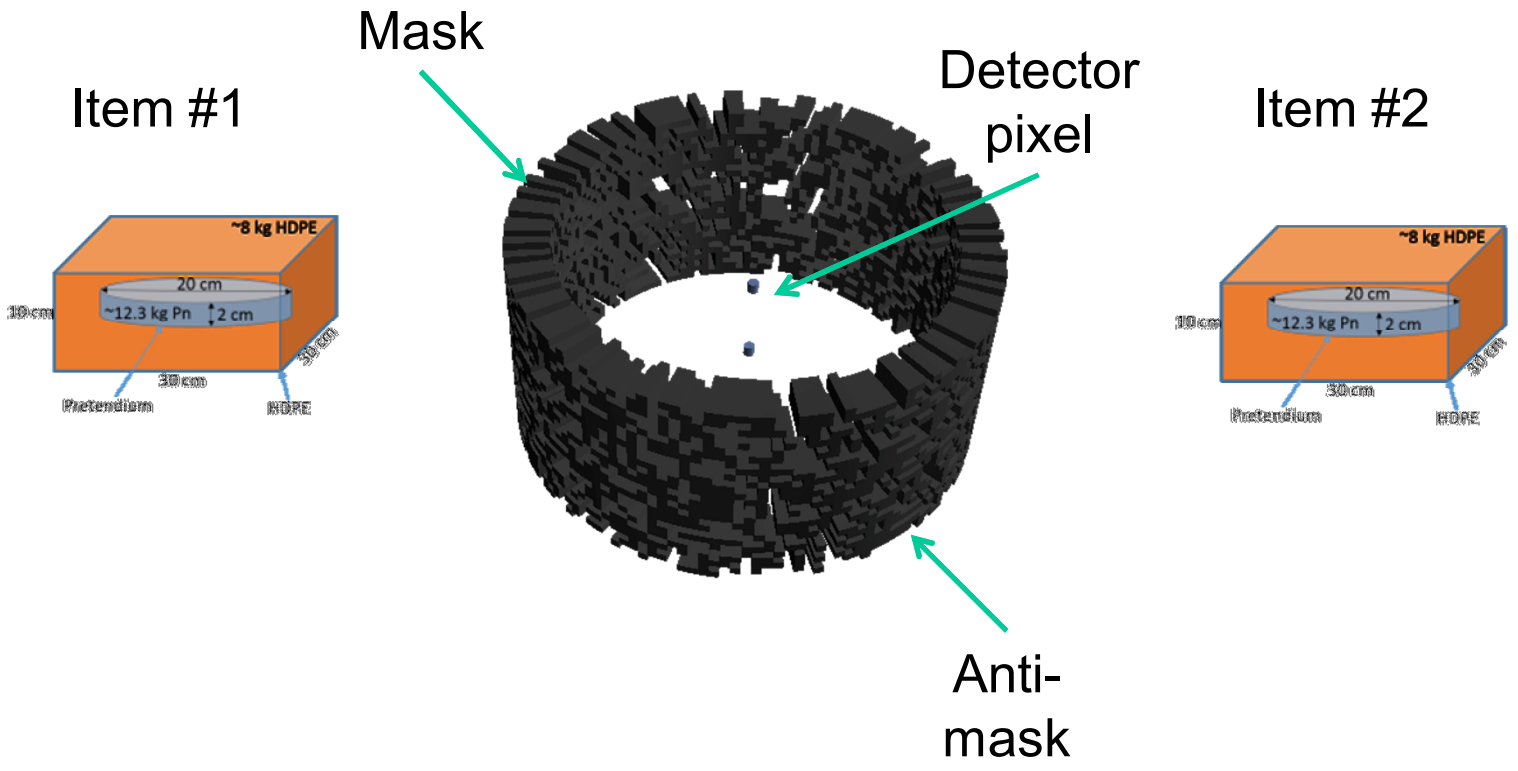
Modulation pattern is unfolded to 2-D image



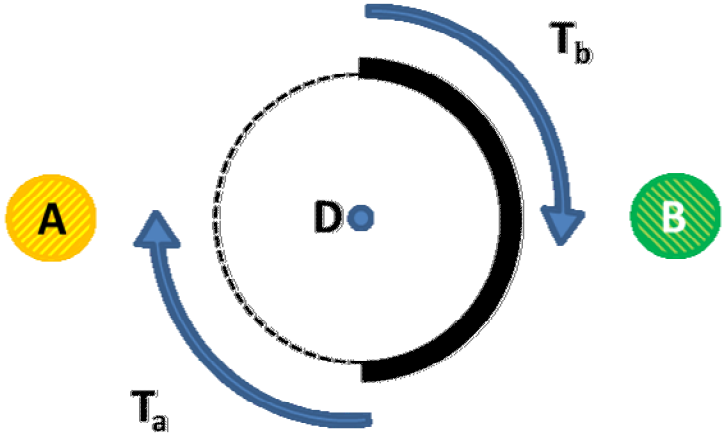
J. Brennan, E. Brubaker, M. Gerling, P. Marleau, K. McMillan, A. Nowack, N. LeGalloudec, M. Sweany, “Demonstration of Two-dimensional Time-encoded Imaging of Fast Neutrons”, Nuclear Instruments and Methods A, 2015

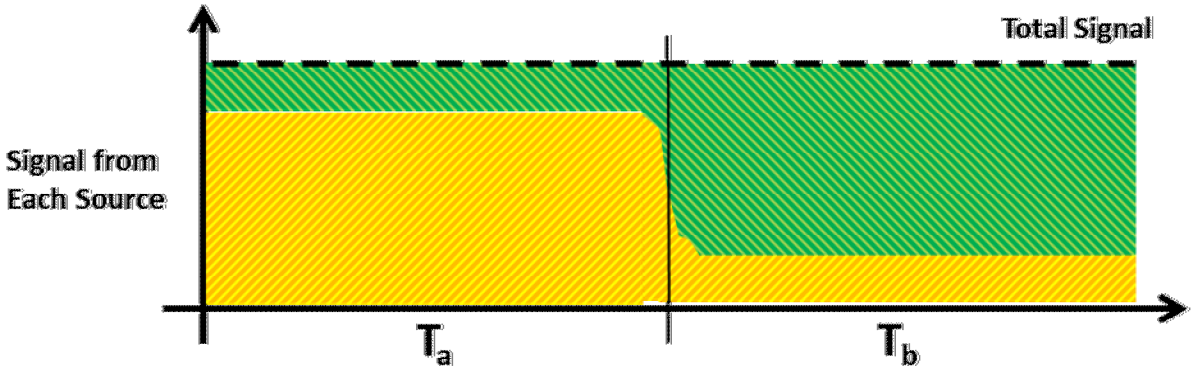
Solution: 2D-TEI mask/anti-mask

If the mask is designed such that one side is the anti-mask of the other, then **Item #2 projects the anti-image of Item #1 at all times if and only if they are identical!**



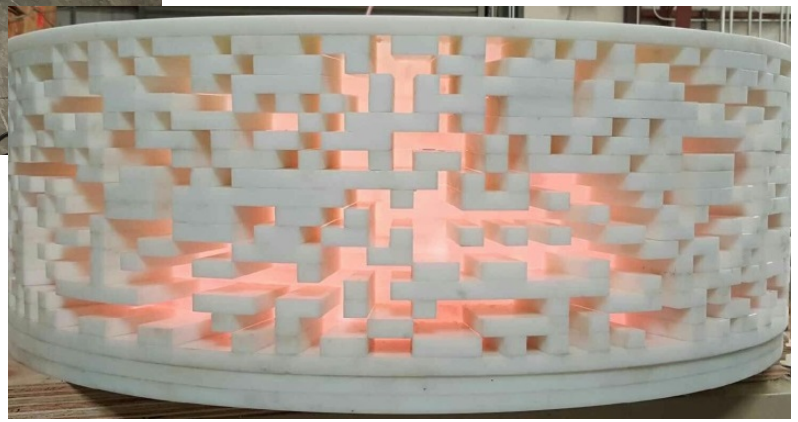
Simple Example of ZKP





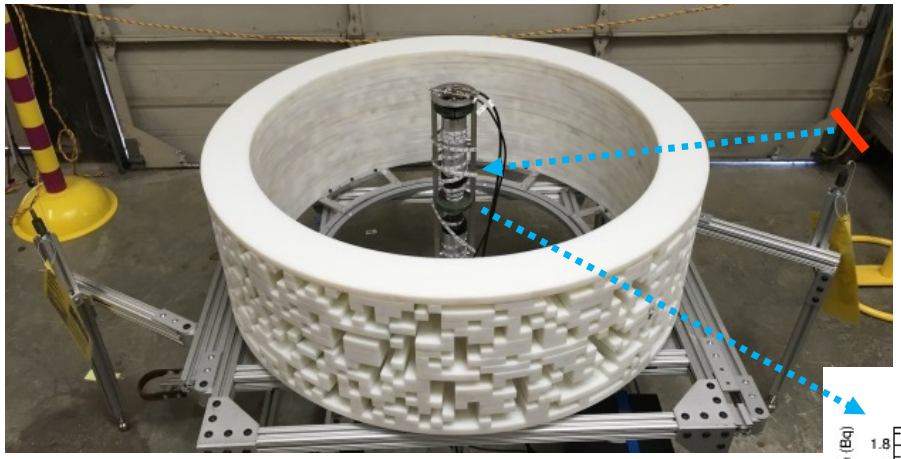
- For example, take a very simple mask: half mask, half aperture.
- The fraction of total count rate coming from A and B is unknown at any given angle.
- In this example, the location (and shape) of the boundary between regions is not revealed.

CONFIDANTE

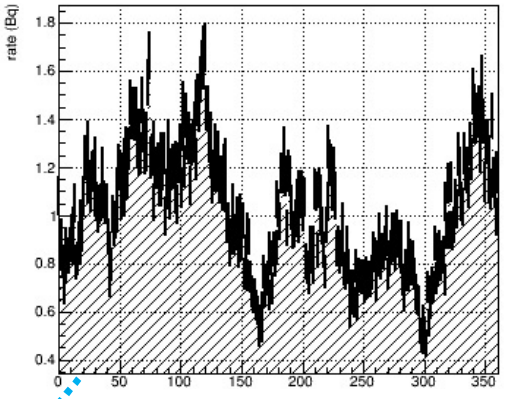


Results: Double Point Source Measurements

Measurement of a double “line” source (~20 hours)

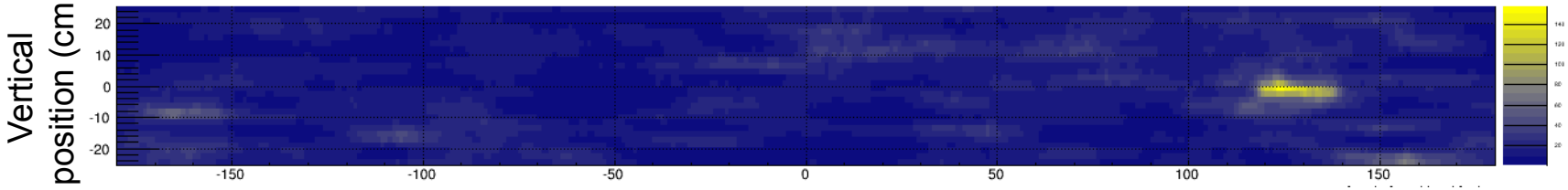


Neutron Rate



Rotation Angle (deg)

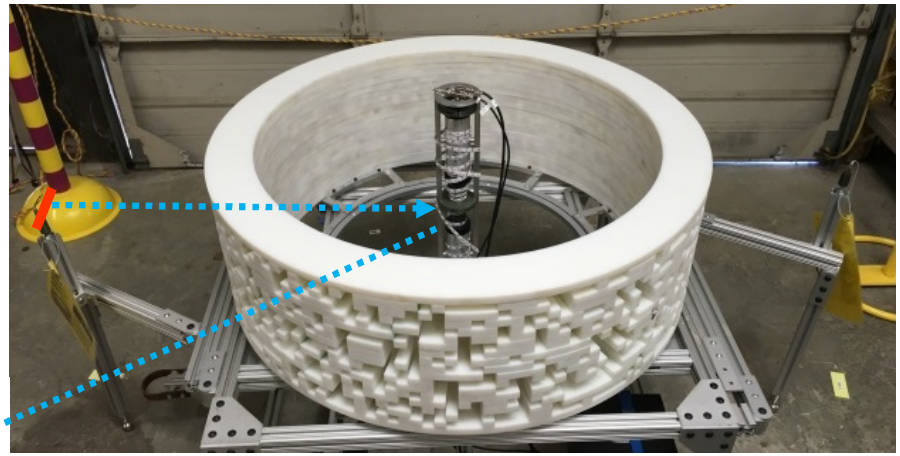
MLEM Reconstruction



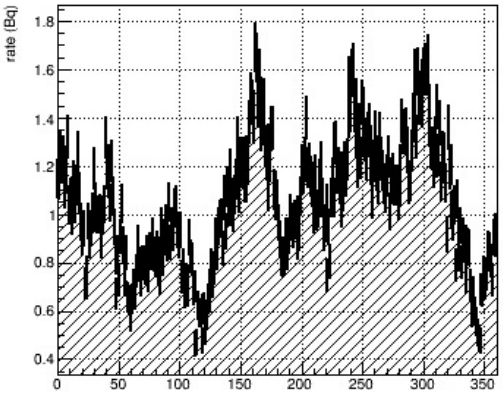
Azimuthal Position (deg)

Results: Double Point Source Measurements

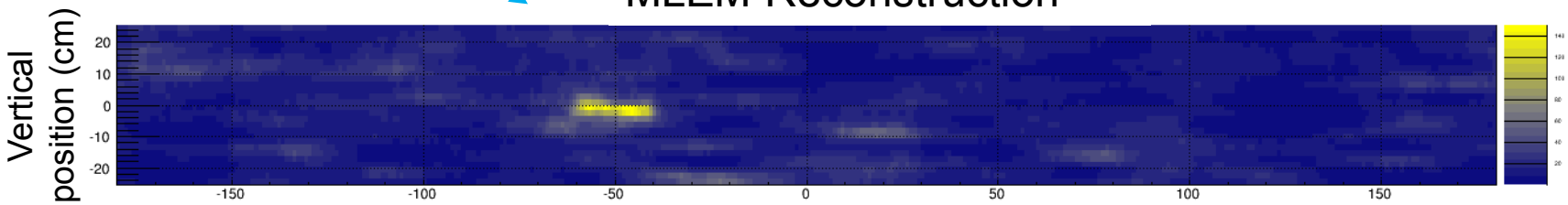
Measurement of a double “line” source (~20 hours)



Neutron Rate

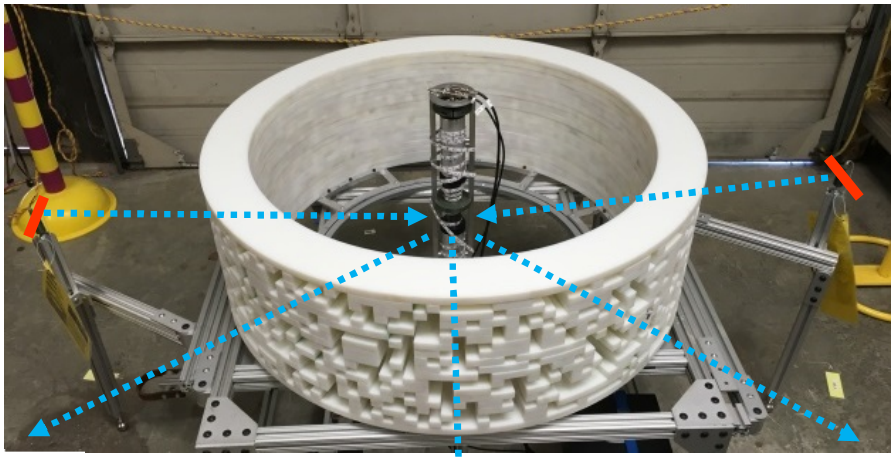


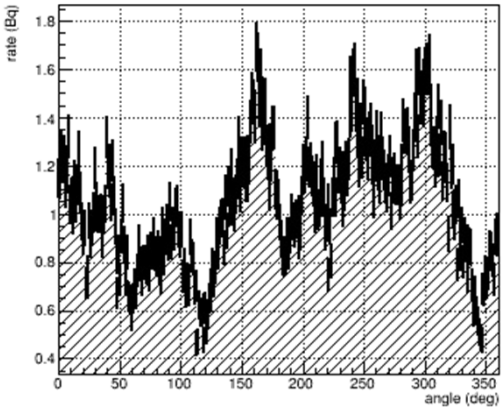
MLEM Reconstruction

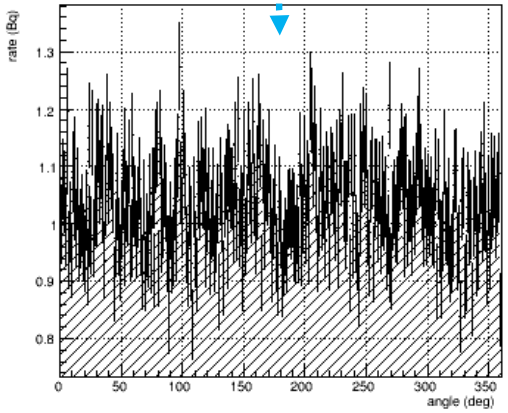


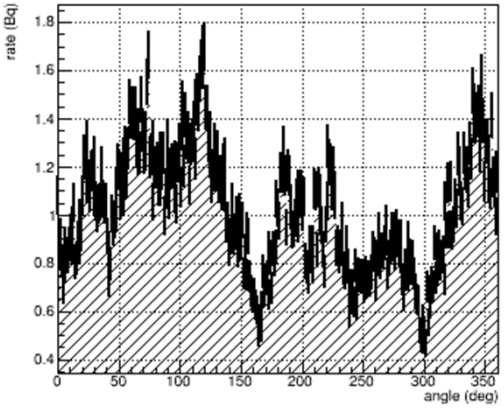
Results: Double Point Source Measurements

Measurement of a double “line” source (~20 hours)



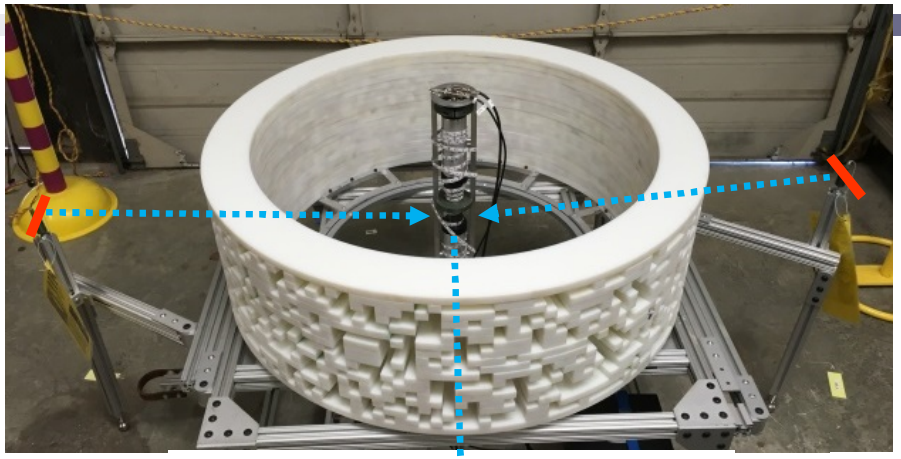






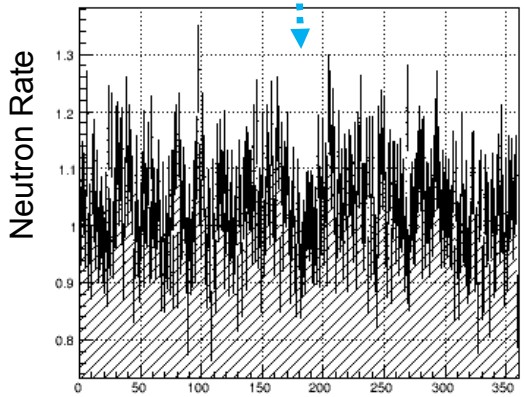
Results: Double Point Source Measurements

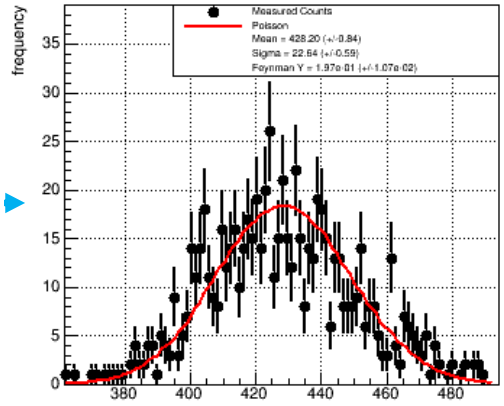
Measurement of a double “line” source (~20 hours total)



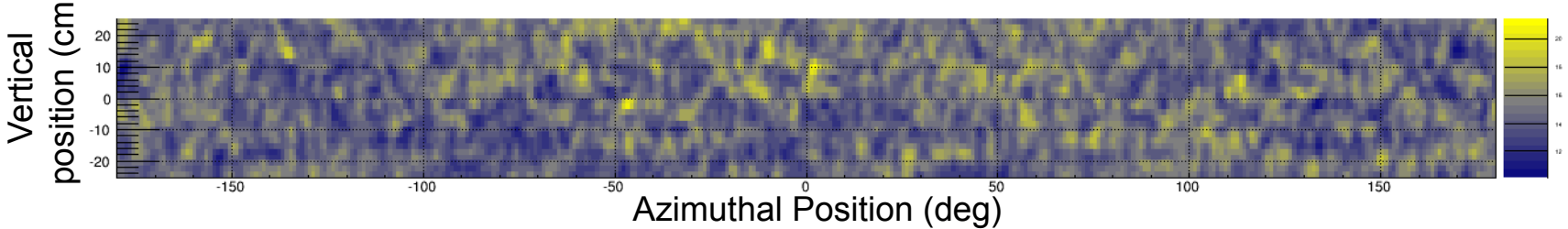
Feynman Y
$= \left(\frac{variance}{mean} - 1\right)$
= 0.197 +/- 0.011

Count Distribution (Poisson – red curve)

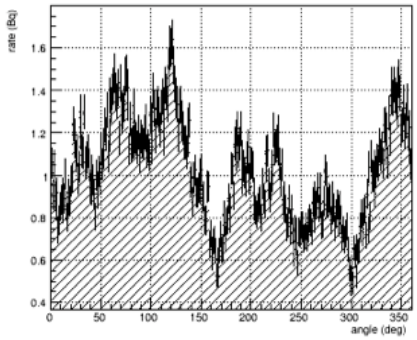


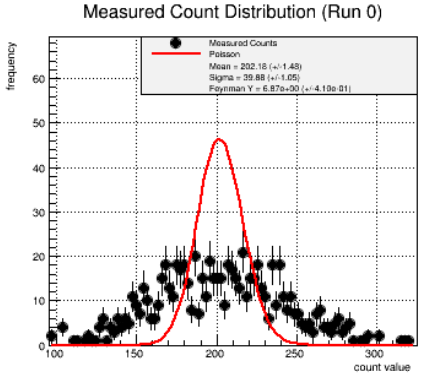


MLEM Reconstruction

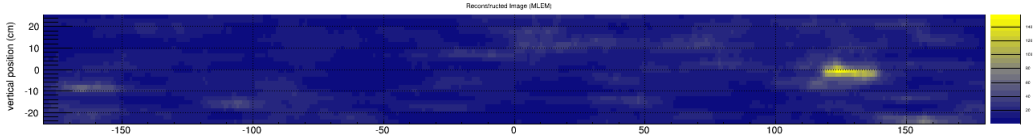


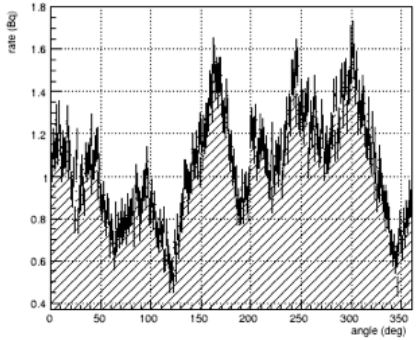
Results: Double Point Source Measurements

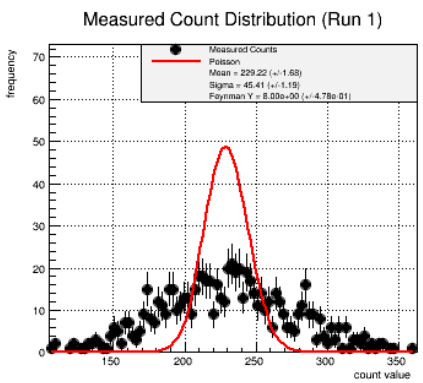




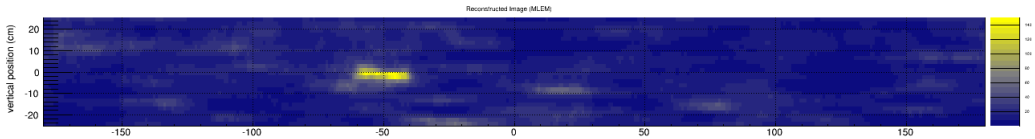
Feynman Y = 6.87 +/- 0.41

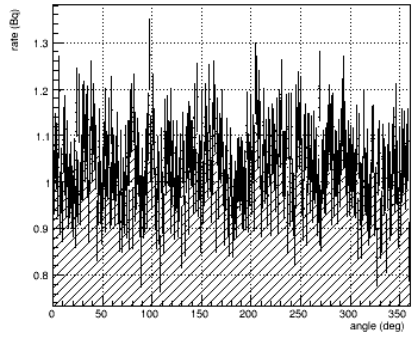


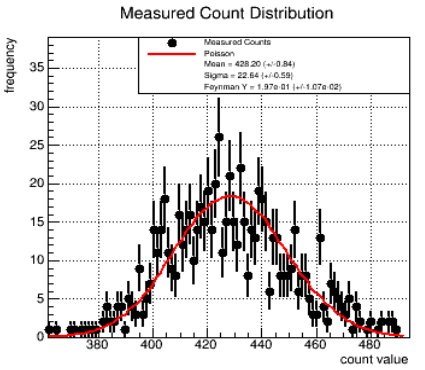




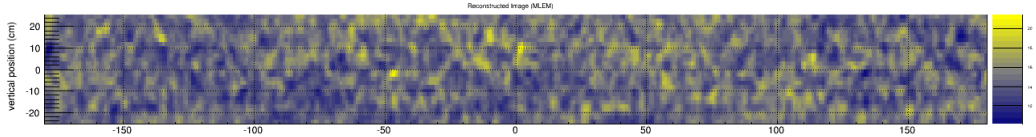
Feynman Y = 8.00 +/- 0.48





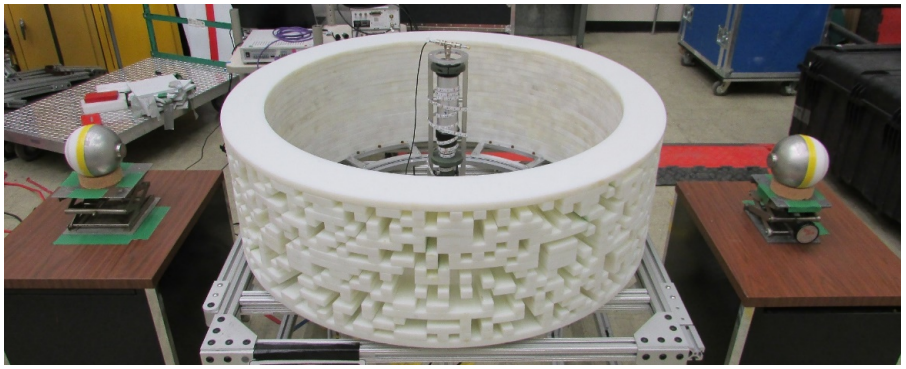


Feynman Y = 0.197 +/- 0.011



Results: LLNL's PuO_2 Hemi Positive Measurement

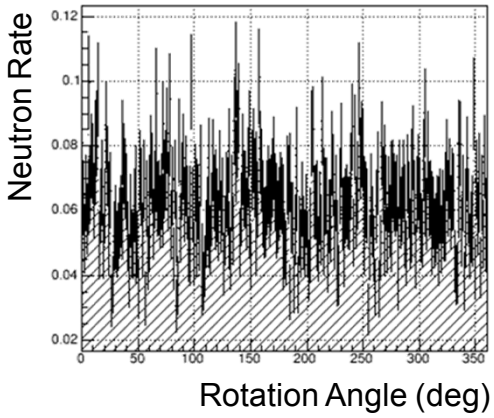
- One hemisphere was placed on each side (180 deg apart) of CONFIDANTE.
- ~68 hours of data was taken.



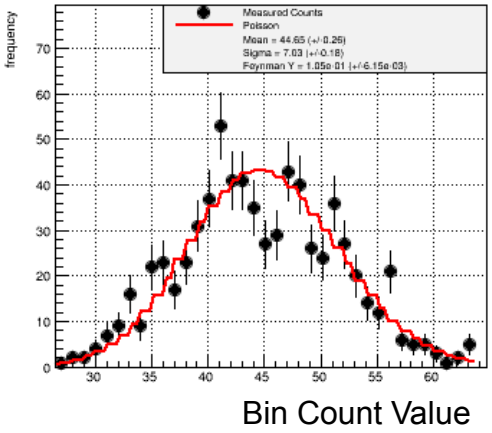
Feynman Y

$= \left(\frac{variance}{mean} - 1\right)$

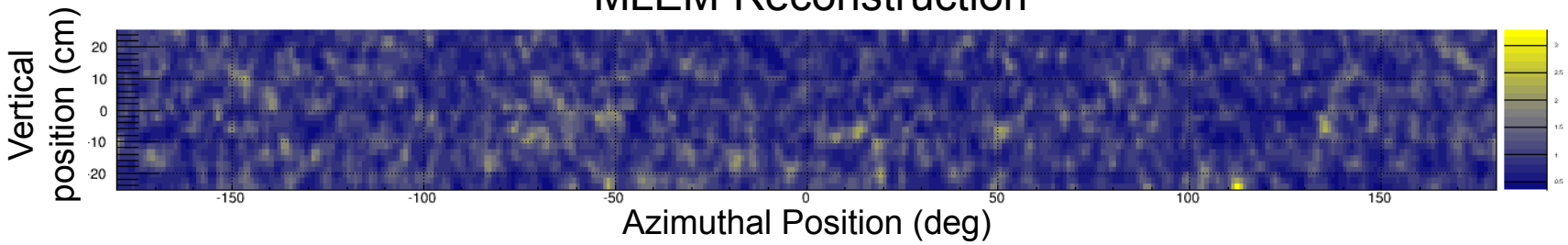
$= 0.105 +/- 0.006$



Count Distribution (Poisson – red curve)

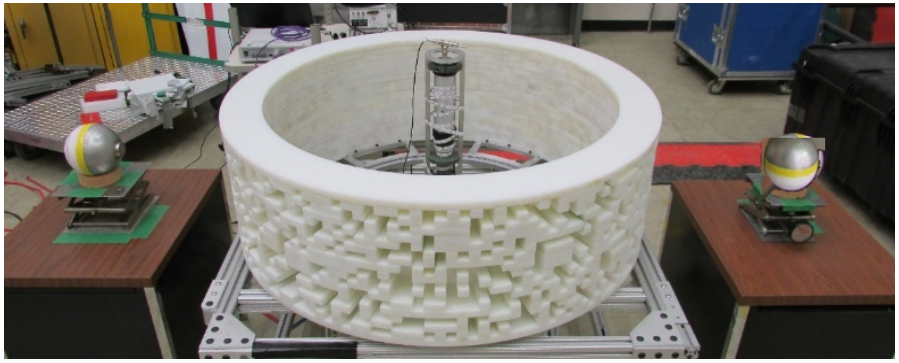


MLEM Reconstruction



Results: LLNL's PuO_2 Hemi Negative Measurement

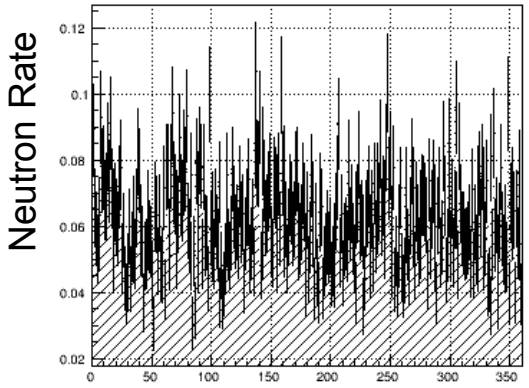
- One hemisphere was placed on each side (180 deg) of CONFIDANTE.
- One was rotated by 90 degrees.
- ~48 hours of data was taken.



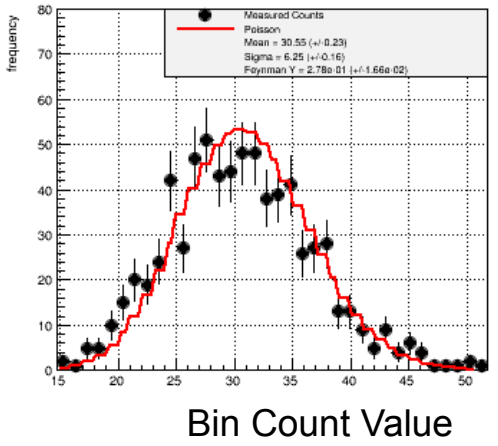
Feynman Y

$= \left(\frac{variance}{mean} - 1\right)$

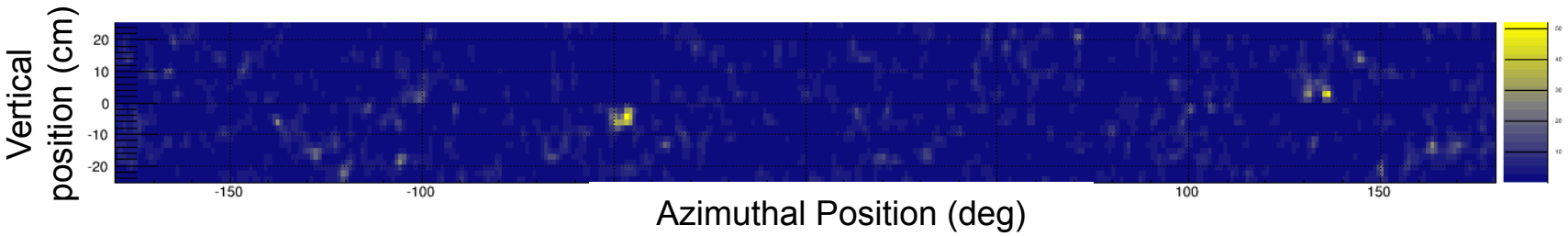
= 0.277 +/- 0.016



Count Distribution (Poisson – red curve)



MLEM Reconstruction



Conclusions

- **Feasibility for the CONFIDANTE concept has been proven.**
- **CONFIDANTE is a simple system based on single pixel compressive imaging.**
- **CONFIDANTE may offer a more easily authenticatable system:**

1. Confirms that two objects are identical in a single measurement with NULL (constant rate) indicating a positive result.

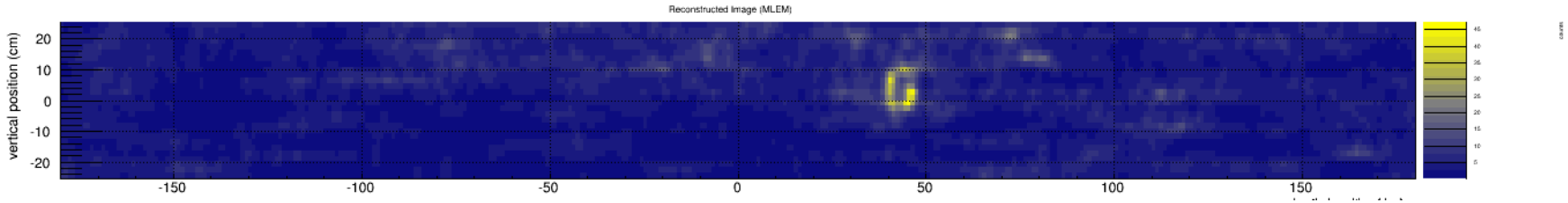
2. Because a NULL (constant rate) is present at all times, the inspecting party might be allowed full access to the measurement and data.

3. A test statistic relating to how “Poisson” that count rate is can be updated to further protect against sensitive information loss.

4. Can image any third inspector provided object during the confirmation measurement without revealing the first two objects as an authentication measure.

Future Work

- **Sensitivity studies**
  - What is the minimum time to verify an object?
  - How exact does the alignment have to be?
  - Is any information revealed with a long measurement or by adding together short measurements?
  - Updating Poisson metric in real time
  - Discrimination between circles and squares of various sizes



- **MCNP simulation (with Patricia Schuster)**
- **Compact gamma-ray version (Patricia Schuster)**

Acknowledgements

This material is based upon work supported by the Department of Energy National Nuclear Security Administration through the Nuclear Science and Security Consortium under Award Number(s) DE-NA0003180 and/or DE-NA0000979.

This presentation was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

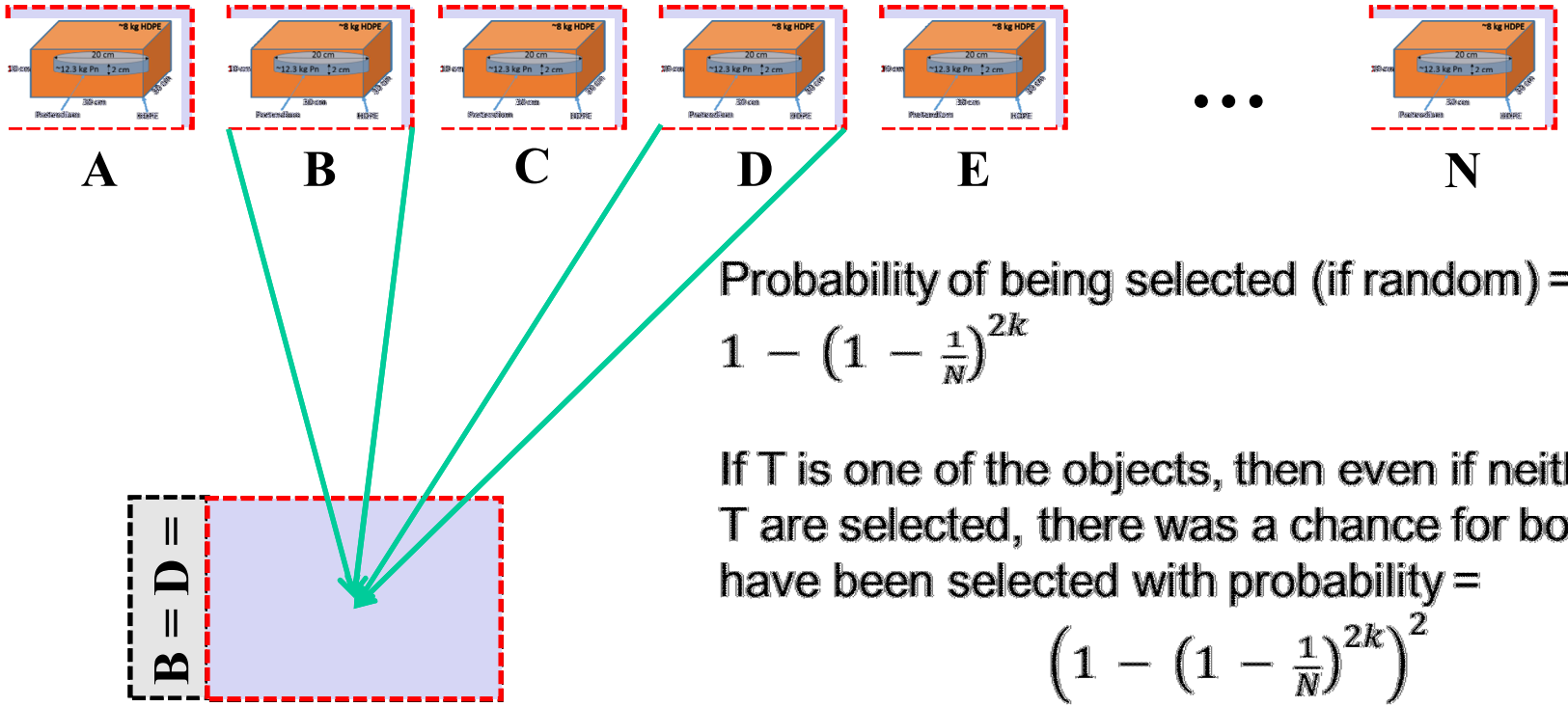
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

This report was prepared with the financial support of the United States Department of State, Bureau of Arms Control, Verification and Compliance (AVC), through the Key Verification Assets Fund, Contract number SAQMMA12M2340. The views, assessments, judgments, and conclusions in this report are the sole representations of the authors and do not necessarily represent either the official position or policy or bear the endorsement of the James Martin Center for Nonproliferation Studies, the Monterey Institute of International Studies, the President and Trustees of Middlebury College, or the U.S. Department of State.

EXTRA SLIDES

CONOPS and Inspector Choice

- The ZKP CONOPS offers an interesting way to gain authentication confidence.
- Presented with N objects and k comparison measurements will be made.



Probability of being selected (if random) =

$$1 - \left(1 - \frac{1}{N}\right)^{2k}$$

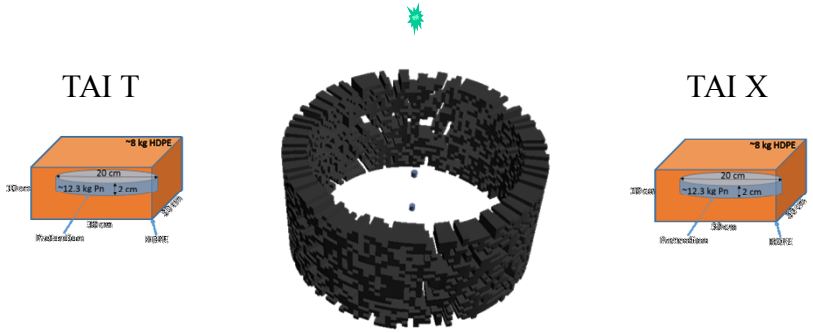
If T is one of the objects, then even if neither X nor T are selected, there was a chance for both to have been selected with probability =

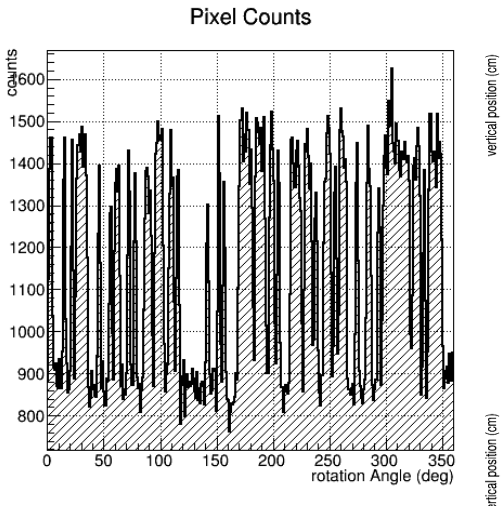
$$\left(1 - \left(1 - \frac{1}{N}\right)^{2k}\right)^{2}$$

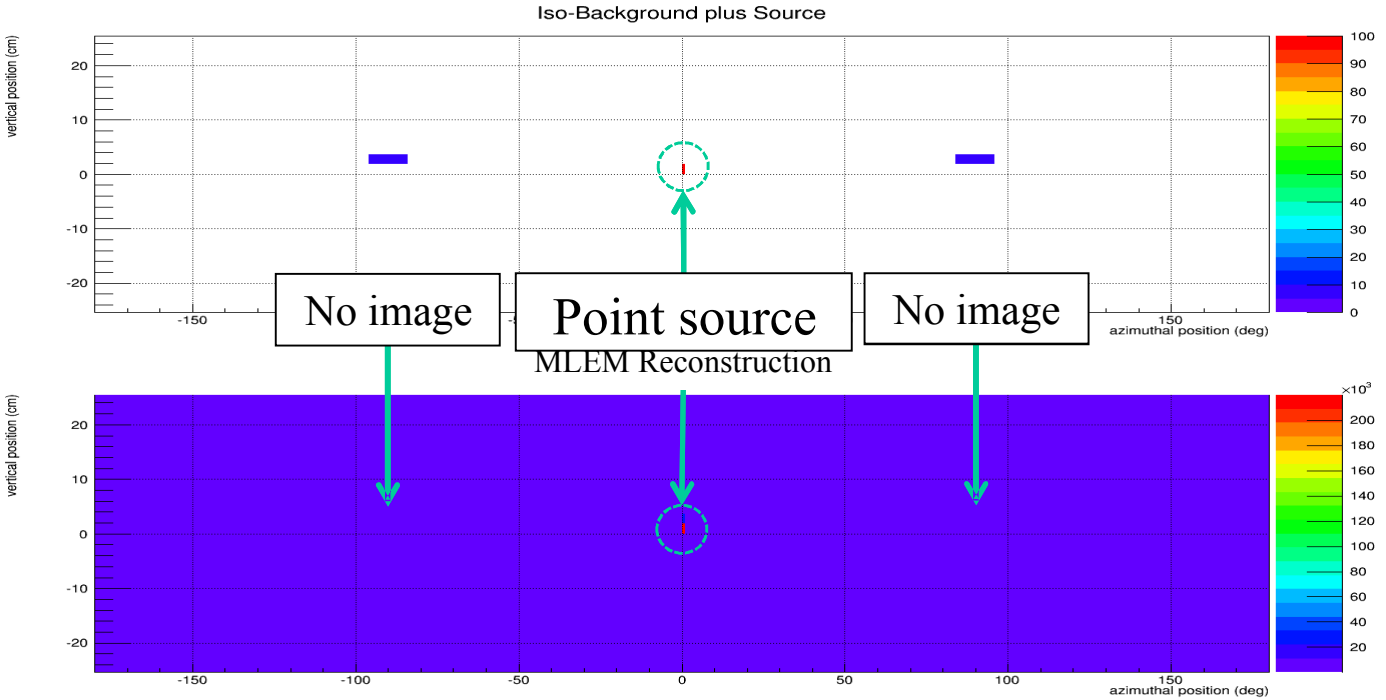
providing some degree of confidence

Verification of Imaging System

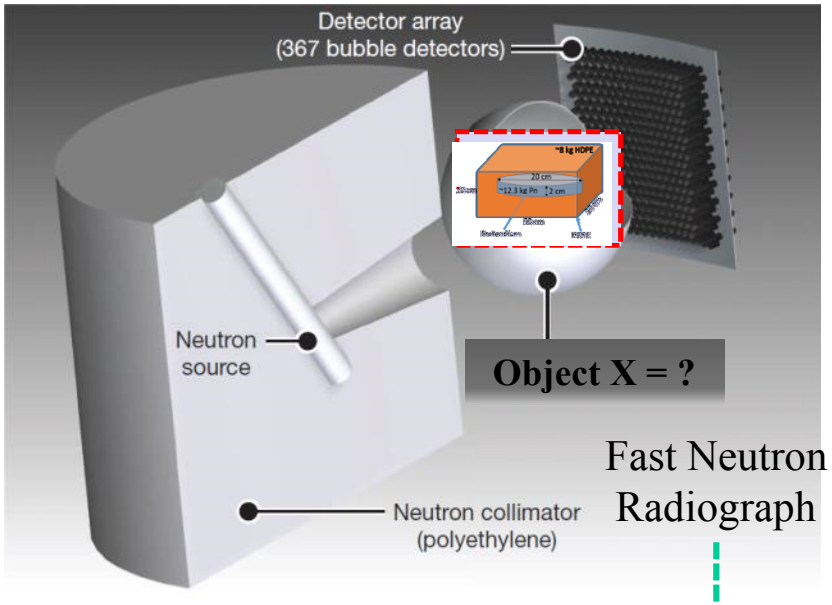
If (and only if) the TAIs are identical, only the third source is visible!



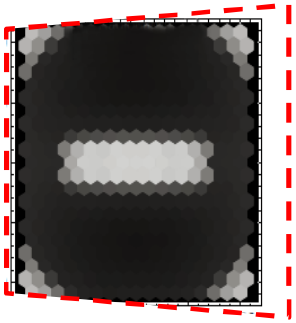




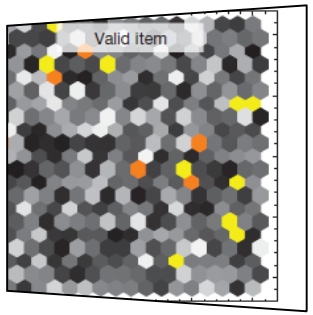
ZKP – Glaser, Barak, and Goldston



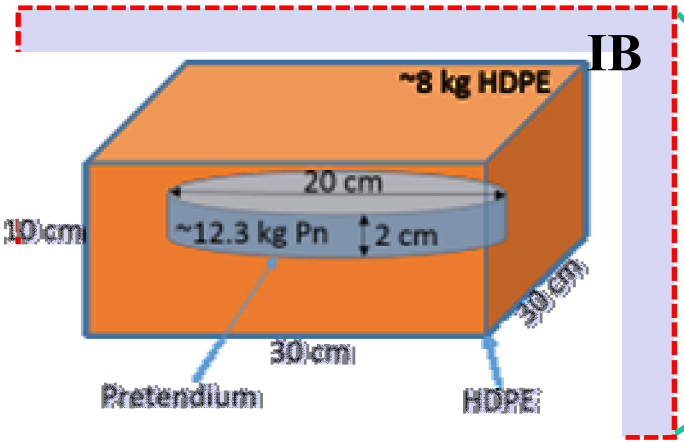
Fast Neutron Radiograph

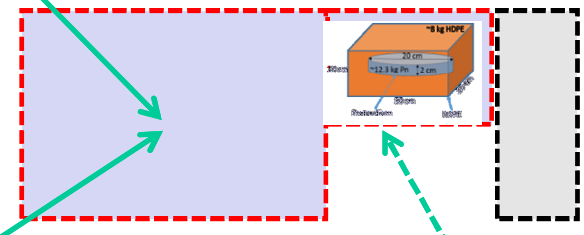


Analog bubble detectors with preloaded complement "template"



Flat featured image (NULL) indicates a true positive.





PASS/FAIL

Preloaded complement behind IB

Images borrowed from: Glaser, Barak, and Goldston, "A zero-knowledge protocol for nuclear warhead verification", doi:10.1038/nature 134557