SAND2017-2464PE

Investigation into Practical Implementations of a Zero Knowledge Protocol: Key Verification Assets Fund Program Review

Peter Marleau

Sandia National Laboratories

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2017-PE

CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding (CONFIDANTE)

Peter Marleau

Sandia National Laboratories

P. Marleau, R. Krentz-Wee, "Investigation into Practical Implementations of a Zero Knowledge Protocol", SAND2017-1649

Outline

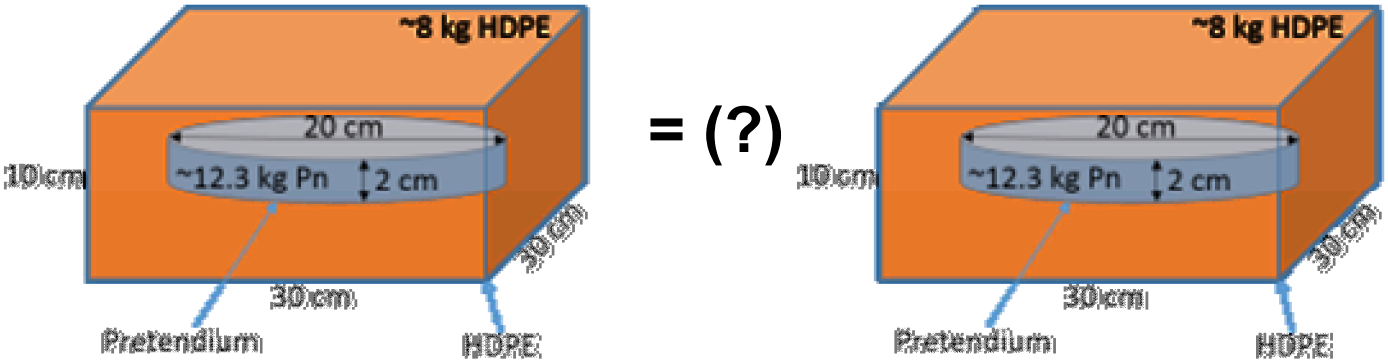
- Authentication and Certification. What's the problem?
- Attribute-based measurements
- Template-based measurements
- Zero Knowledge – what does it buy you?
  - Is this better than a template?
- Comparison Measurements – a new CONOPS?
- Two-dimensional time-encoded imaging
- CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding (CONFIDANTE)
- Measurement campaign results – it works!

Sandia National Laboratories

What's the problem?

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 = ?

Sandia National Laboratories

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

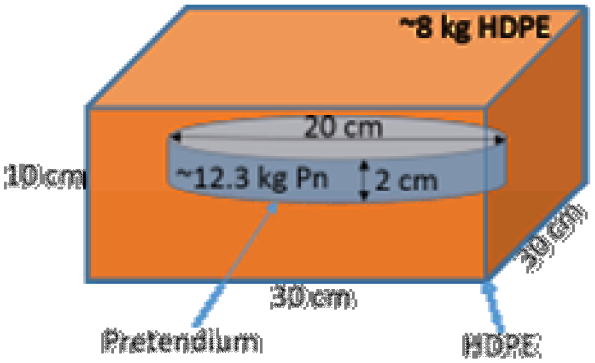
Can we measure it?

Authentication

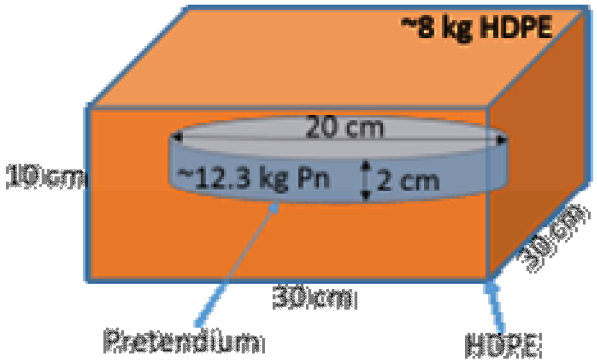
- Measurement must be relevant
- Measurement must be specific

Certification

- Measurement must not do more than required.
- Most distinguishing characteristics imply design/sensitive information.



= (?)



Object T = valid type 1 TAI

Object X = ?

Sandia National Laboratories

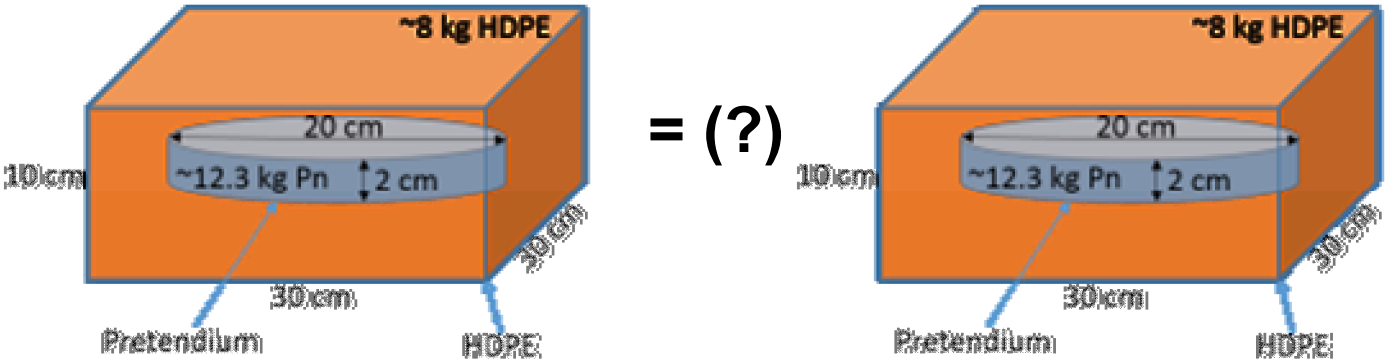
Specificity through attributes?

Authentication

- Relevant and specific attributes can be defined.
- Attributes can be derived from measurements.

Certification

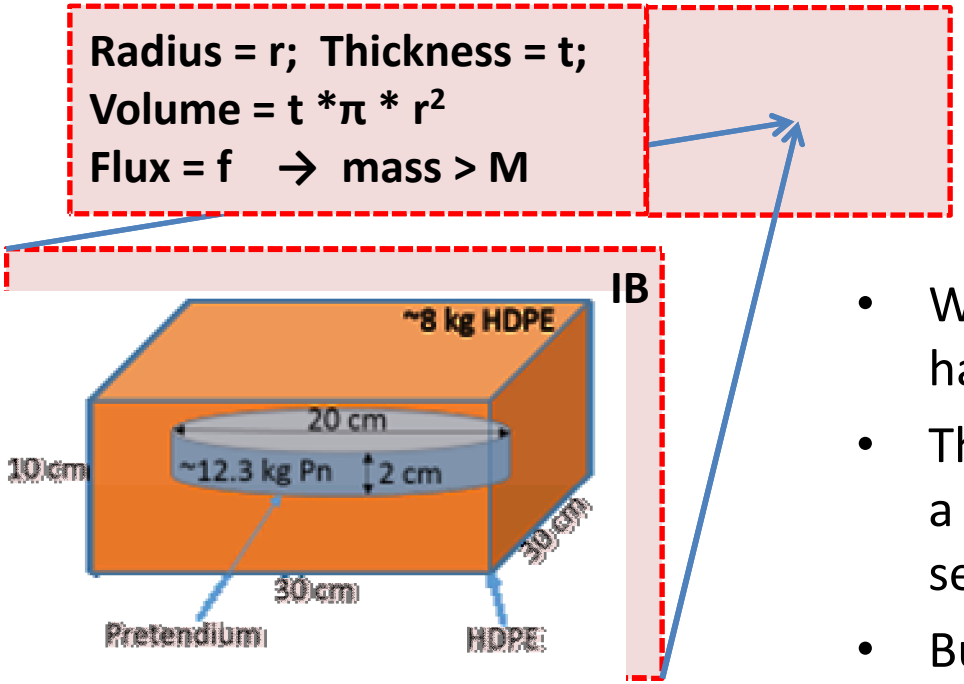
- Acceptable threshold values must exist.
- Extraneous information must be limited or protected -> IB



Object T = valid type 1 TAI

Object X = ?

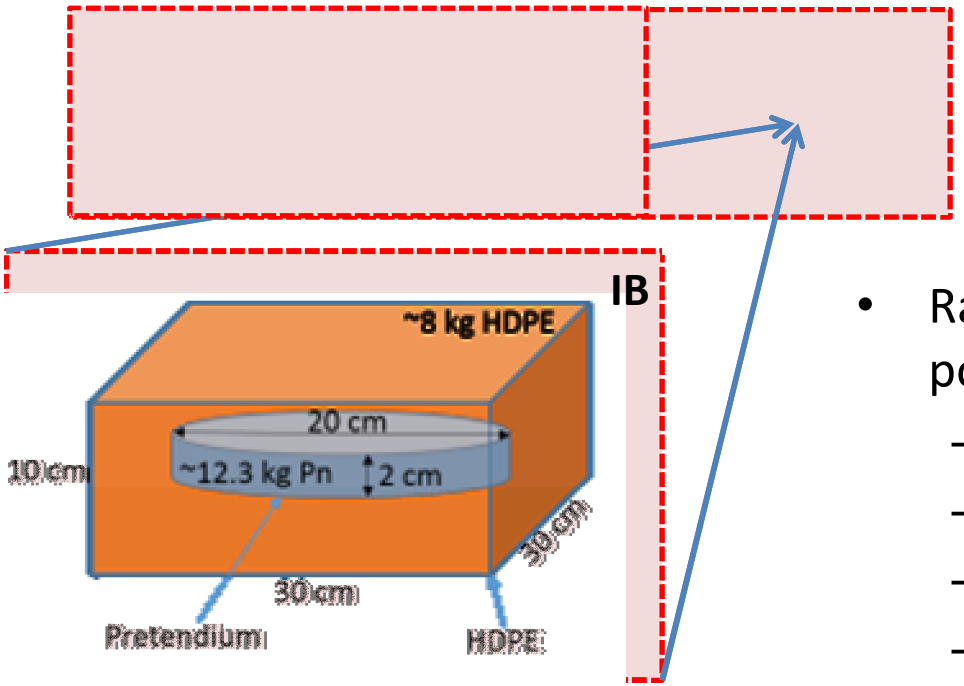
Attributes – necessitate an IB



Object T = valid type 1 TAI

- We could declare that Object T has an attribute (I.e. mass > M)
- This defines what it means to be a TAI without carrying around sensitive information.
- But the measurement and calculation will probably reside behind an information barrier (IB) …

Attributes – necessitate an IB



Object T = valid type 1 TAI

- Radiation imaging accesses many possible attributes:
  - Shape
  - Size
  - Composition
  - Mass
  - Intervening material
  - Etc. Etc.
- But calculations can be quite intensive.

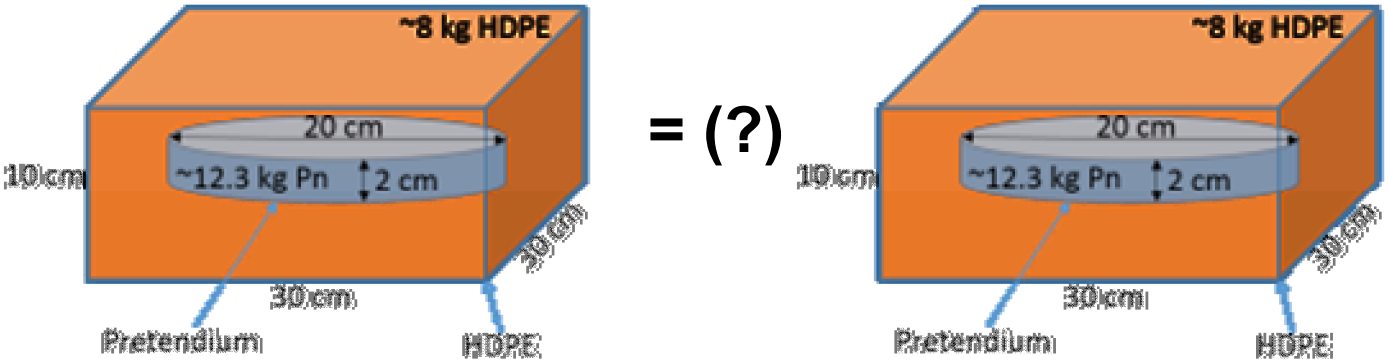
Specificity through templates?

Authentication

- Relevant and specific attributes can be defined by what is measured by a system ***without complicated analysis!***

Certification

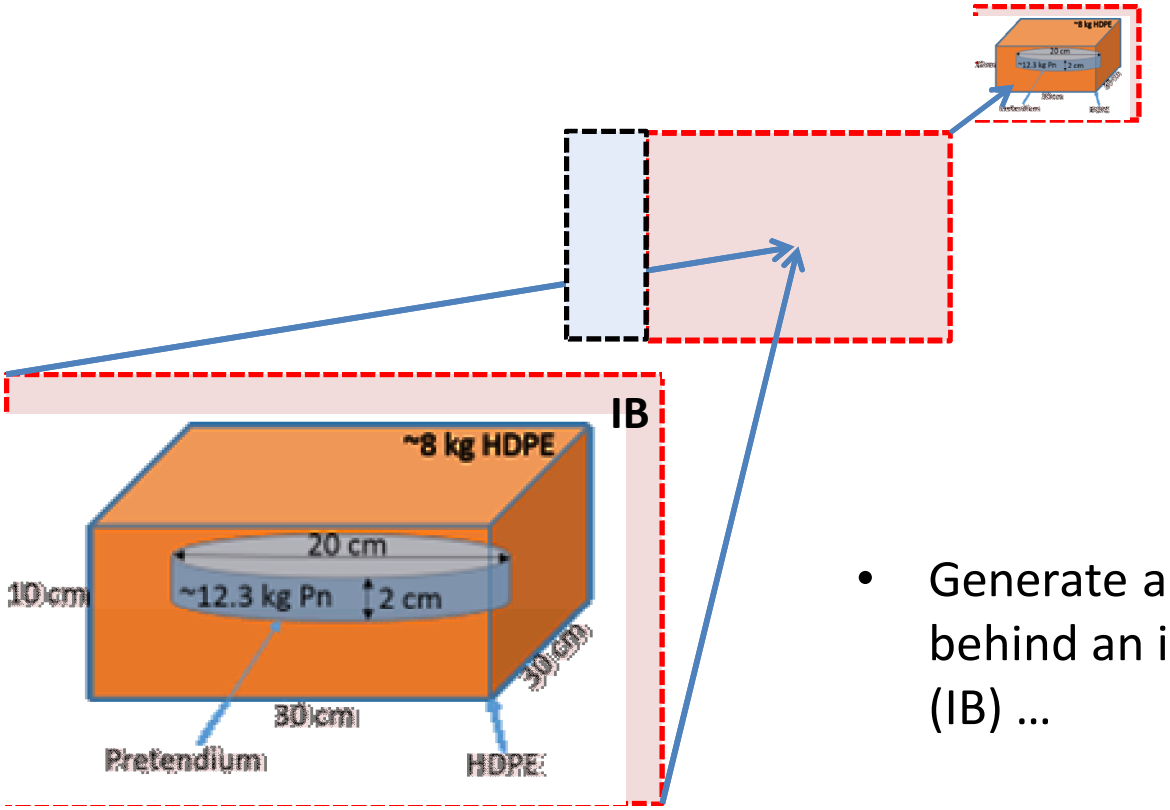
- Must sequester data if superfluous/sensitive information can be derived from data.



Object T = valid type 1 TAI

Object X = ?

Traditional Templates - generation

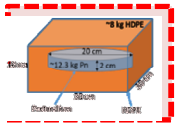


Object T = valid type 1 TAI

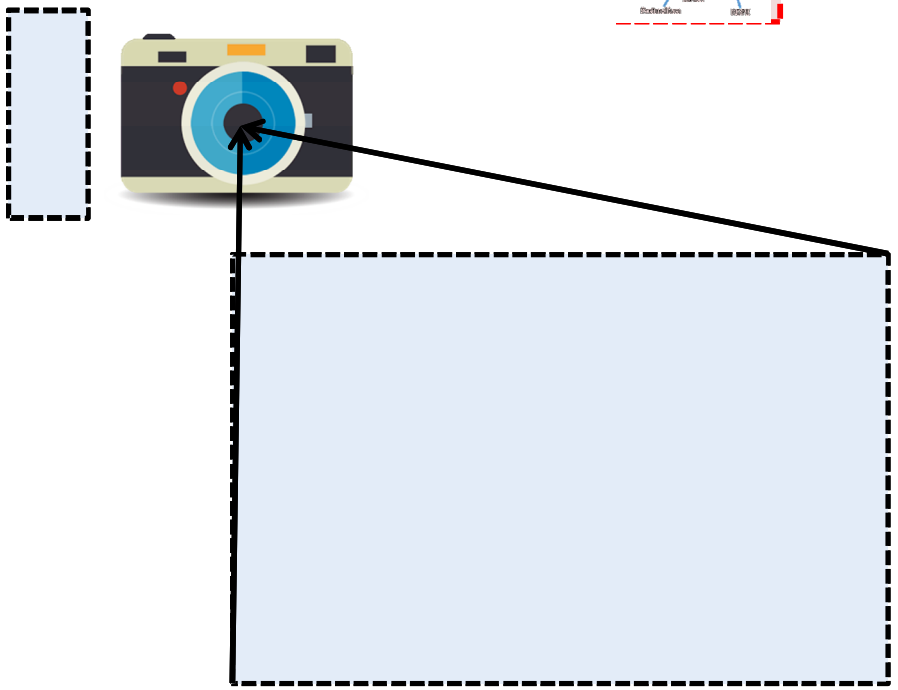
- Generate a template/data behind an information barrier (IB) …

Traditional Templates - authentication

- Sequester template/data which may be sensitive
- Authenticate equipment …



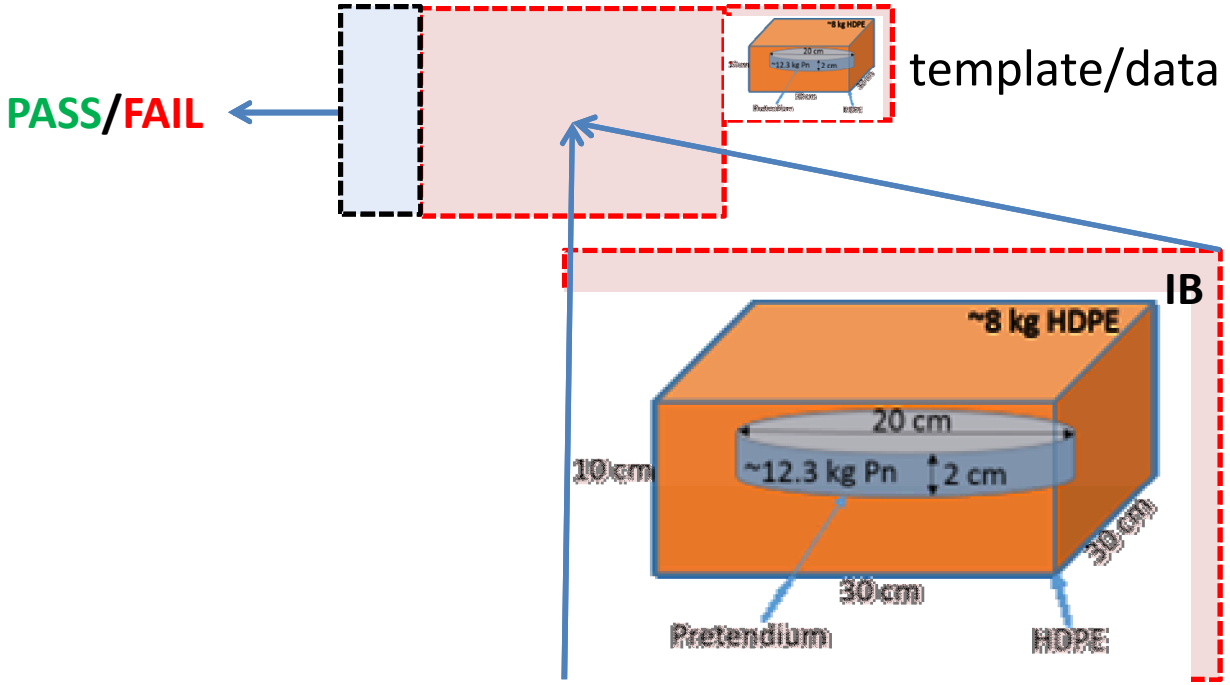
template/data



Object Z = ?

Traditional Templates - comparison

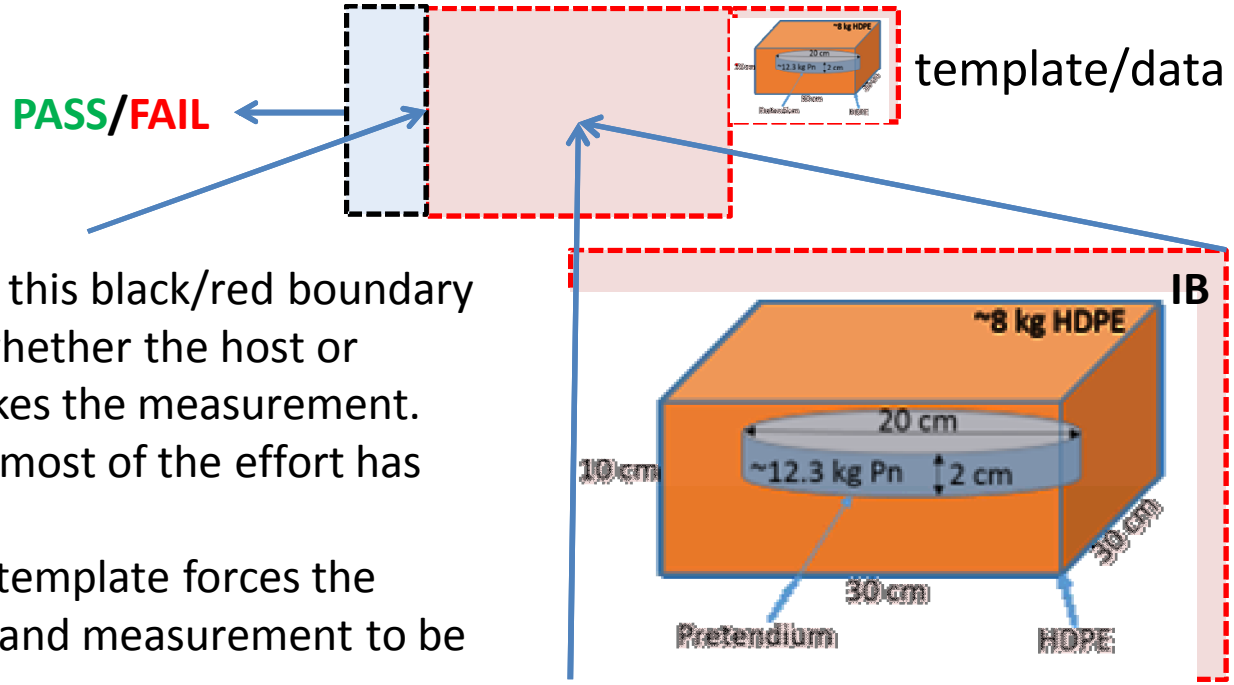
- Measure object declared to be of like type.
- Analysis is simple; does the data match within expected uncertainties?



Object X = ?

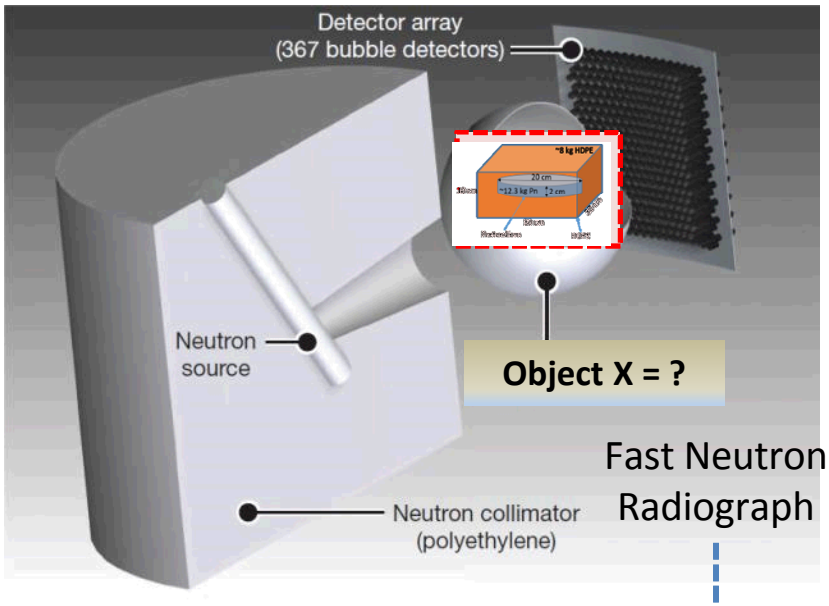
Templates – who measures?

- Who makes the measurement? Is the measurement itself authenticatable?

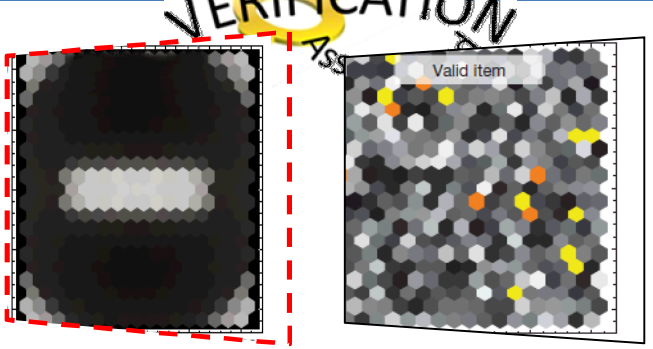


- The nature of this black/red boundary determines whether the host or inspector makes the measurement.
- This is where most of the effort has gone.
- At worst, the template forces the entire device and measurement to be behind an IB.

ZKP – Glaser, Barak, and Golston

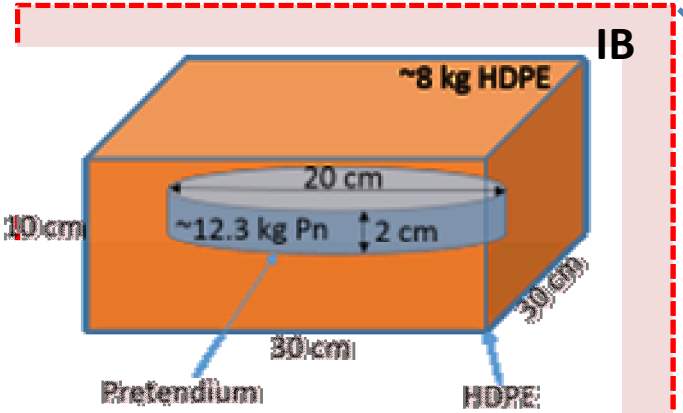


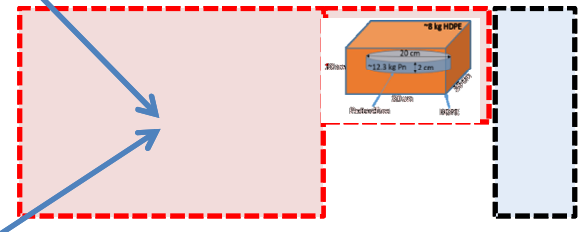
Fast Neutron Radiograph



Analog bubble detectors with preloaded complement "template"

Flat featured image (NULL) indicates a true positive.





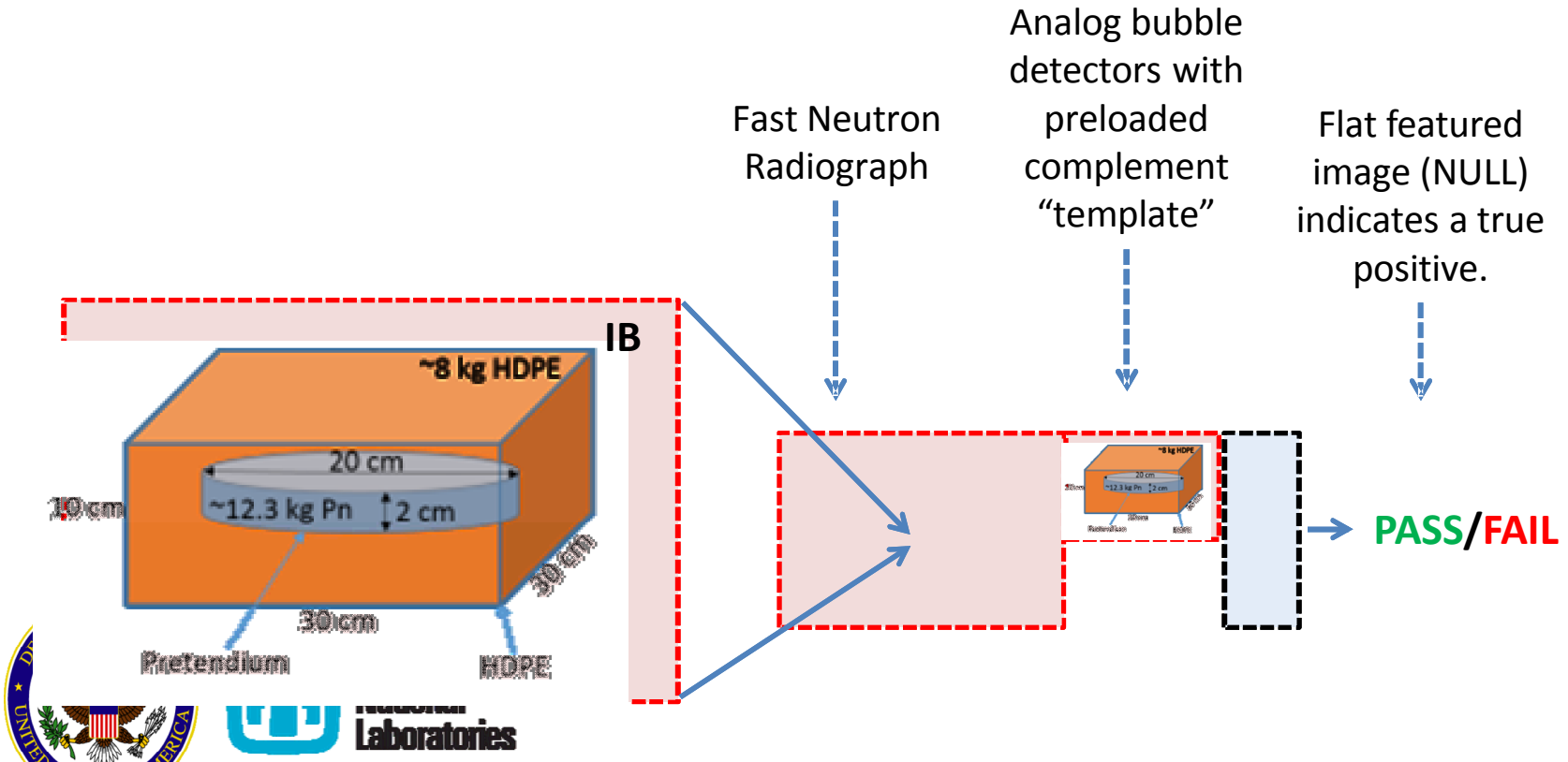
PASS/FAIL

Has this boundary moved?

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

ZKP – authentication measures

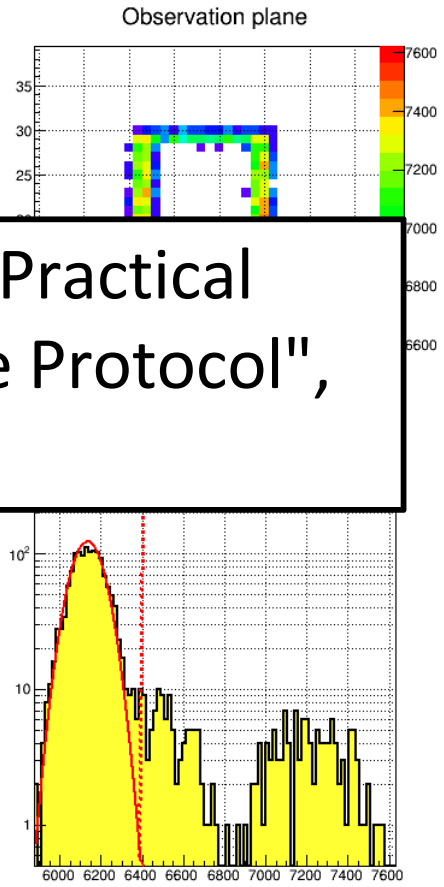
- Research Questions
  - Is there anything that we can do to make this more authenticatable?
  - Can we share the rates in a subset (up to all) of the detector pixel counts with spatial information removed before/during/after the measurement?
  - **What sensitive information is at risk?**



Rectangular Source Counts

VERIFICATION

- 8.57e6 counts represented in Gaussian.
- 1.43e6 counts in source.



See Final Report: "Investigation of Practical Implementations of a Zero Knowledge Protocol", SAND2017-1649

- There are 230 pixels to the right of the threshold. Therefore these excess source counts are distributed across an object of this **total angular size**.

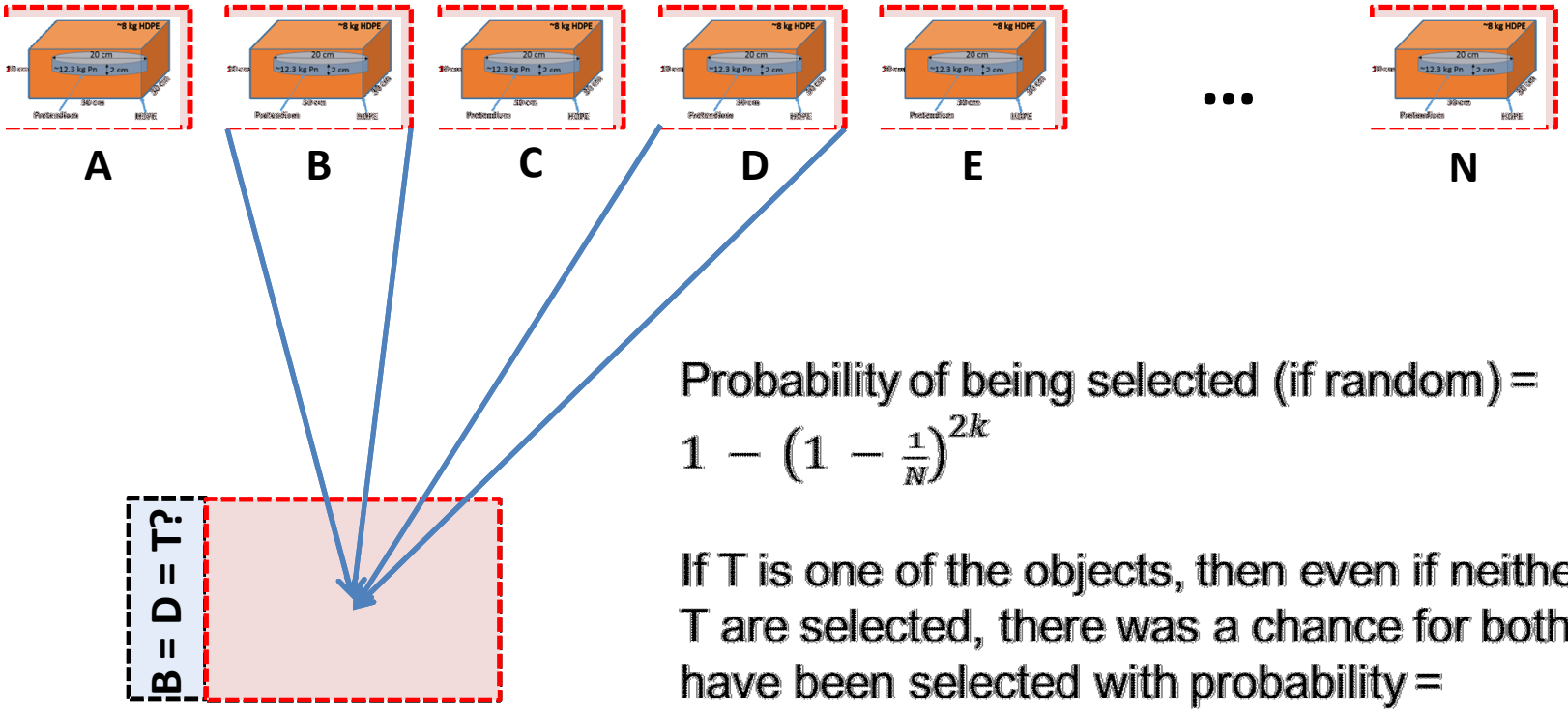
- What else can we learn? What can the shape of the distribution tell us? Have we gone far enough?

$\rightarrow$ ***Classified Study***

Sandia National Laboratories

ZKP – 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) =

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

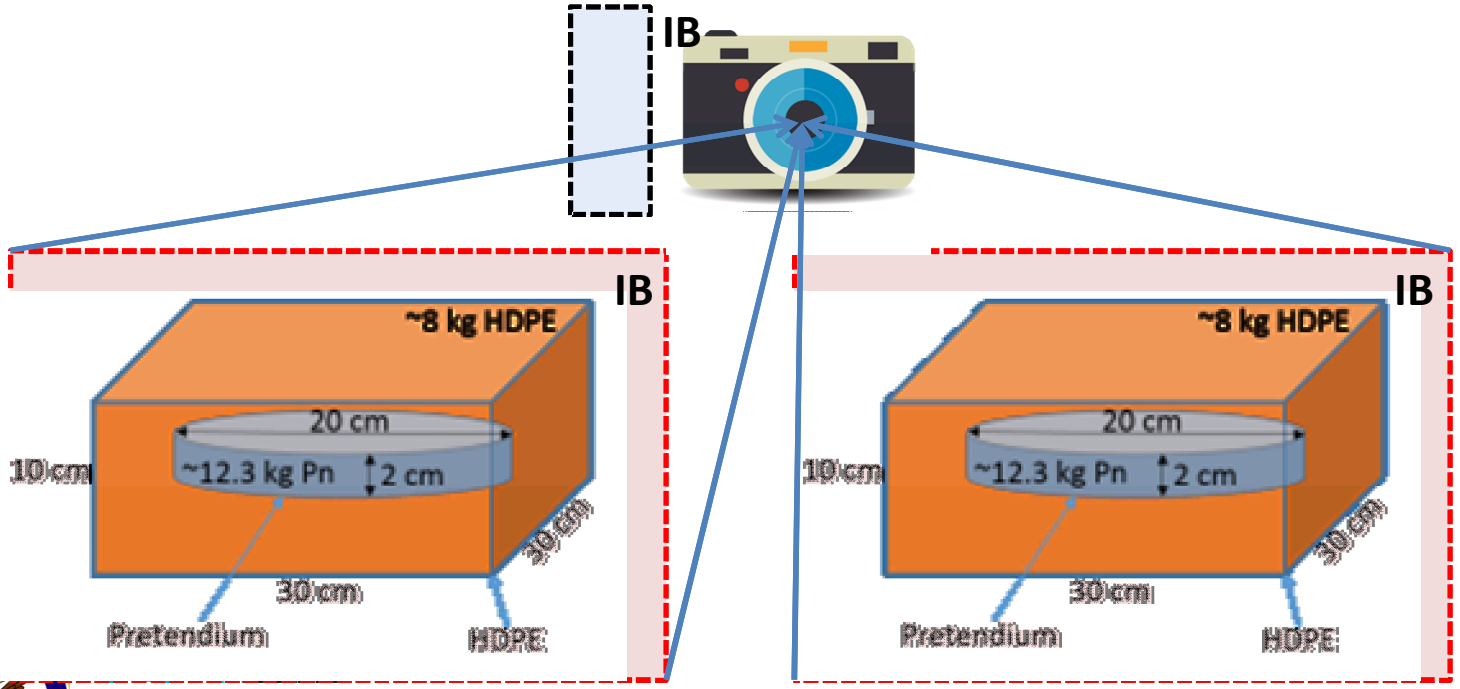
If T is one of the objects, then even if neither X nor T are selected, there was a chance for both to have been selected with probability =

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

providing some degree of confidence

Zero Knowledge comparison measurement?

- Is there a physical implementation of the confirmation measurement that the inspector can watch and authenticate?
- **It would be great if we could get a physical NULL as an indication of positive confirmation at all times, *not just at the end*.**

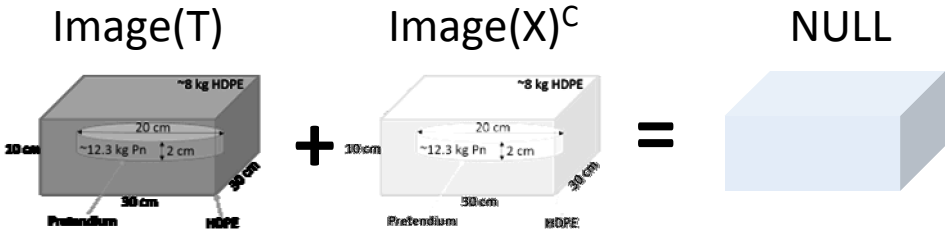


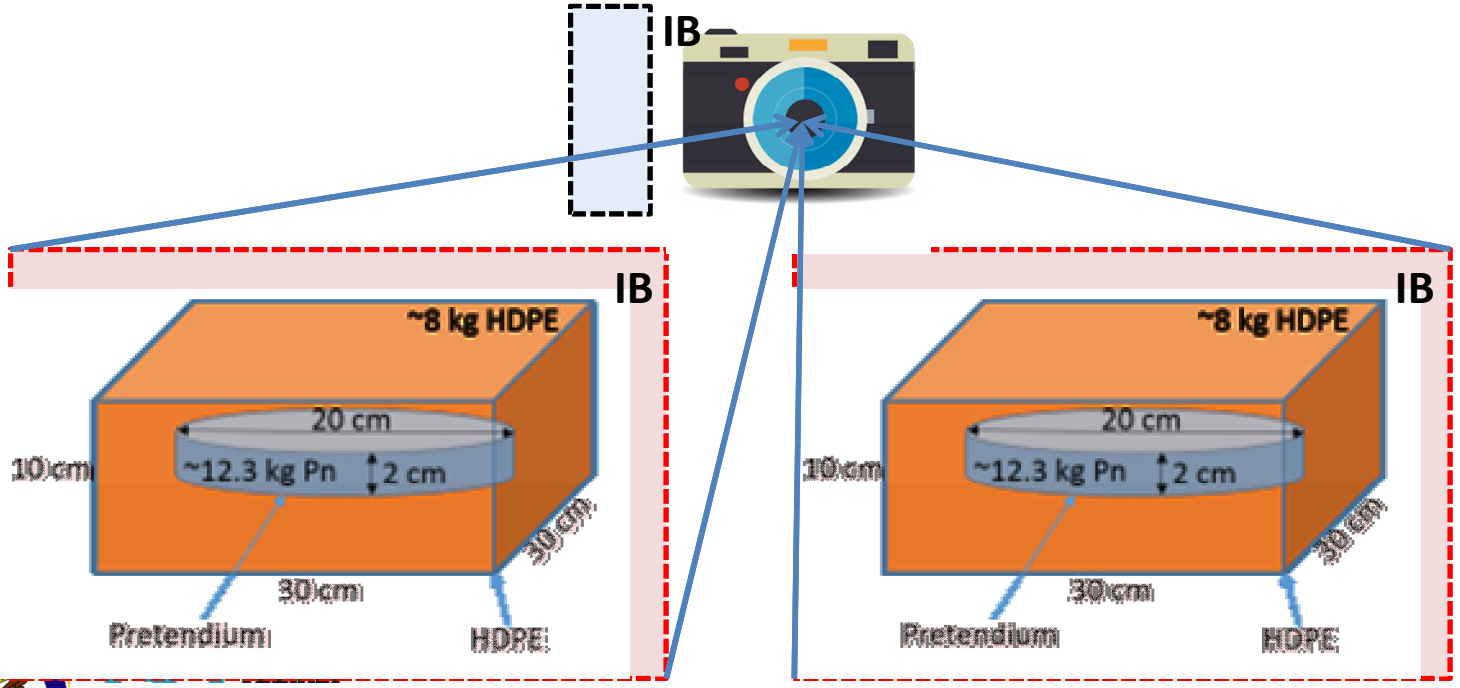
Object T = valid type 1 TAI

Object X = ?

Proposal – complementary comparison

- What we need is to turn one image into its complement ***at all times***.

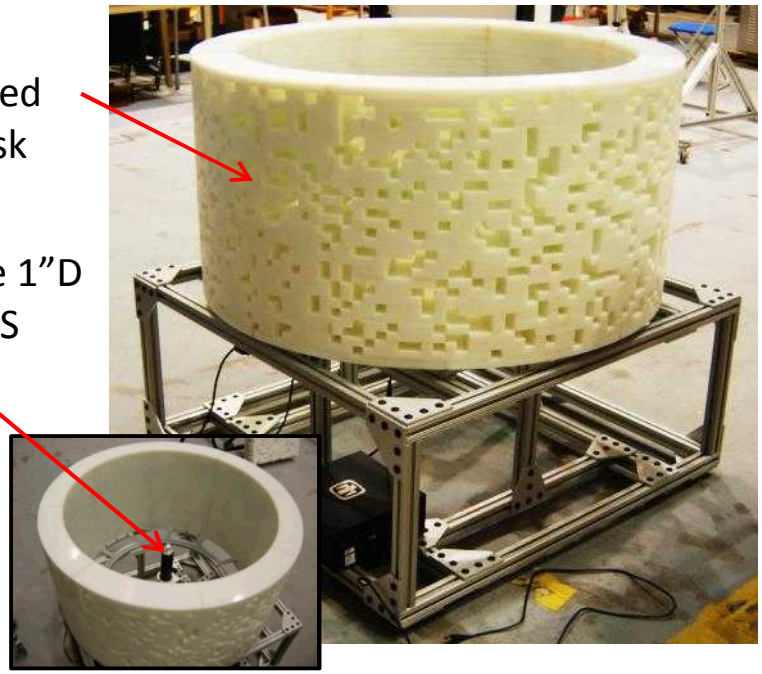




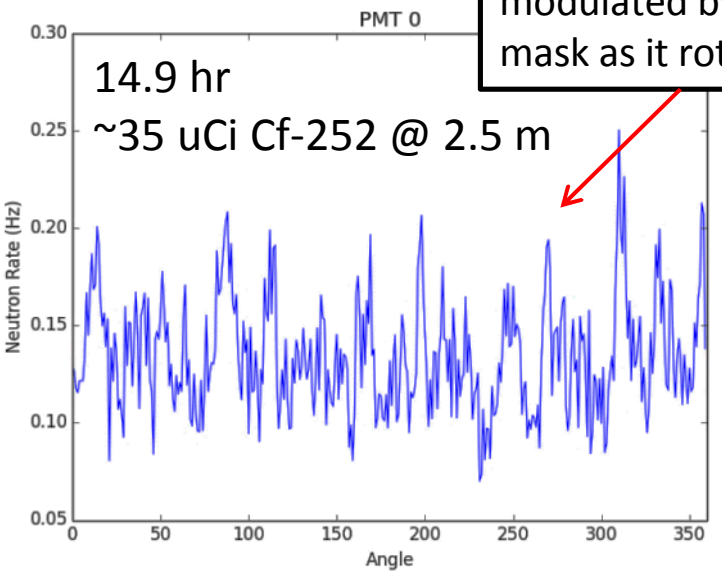
2D Time-encoded Imaging (TEI)

2-d coded mask

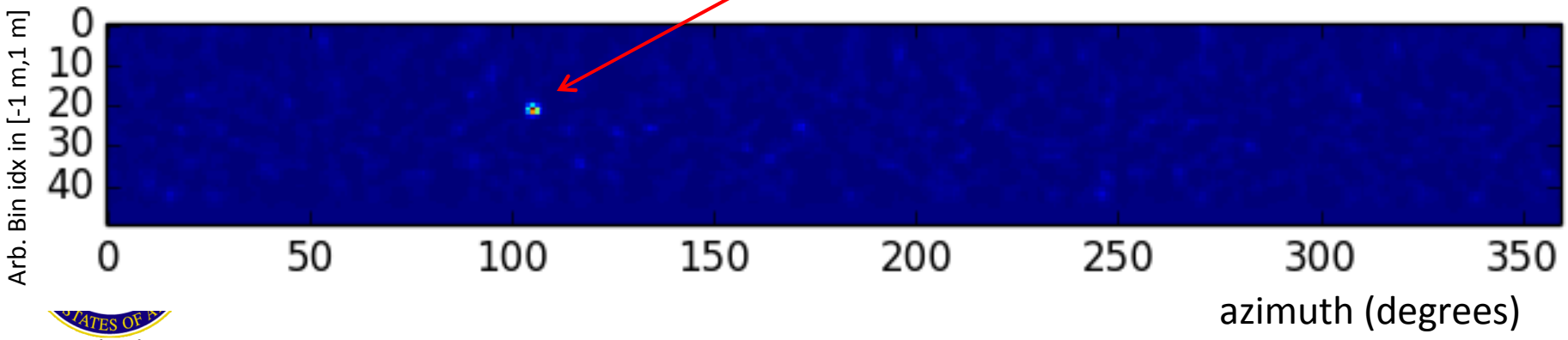
Single 1”D x 1” LS pixel



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



Modulation pattern is unfolded to 2-D image

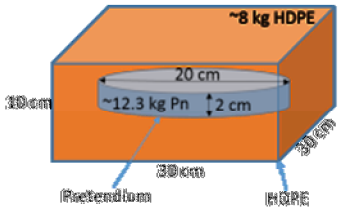


J. Brennan, E. Brubaker, M. Gerling, P. Marleau, K. McMillan, A. Nowack, N. LeGalloudec, M. Sweany, “Demonstration of Two-dimensional Time-encoded Imaging of Fast Neutrons”, Nuclear Instruments and Methods A, 2015

Here's where the magic happens …

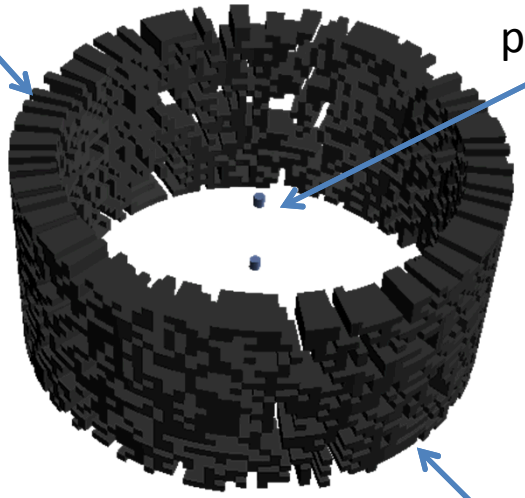
If the mask is designed such that one side is the anti-mask of the other, then **TAI #2 projects the anti-image of TAI #1 at all times if and only if they are identical!**

TAI #1



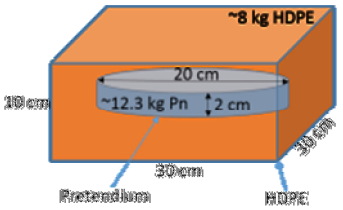
Mask

Detector pixel



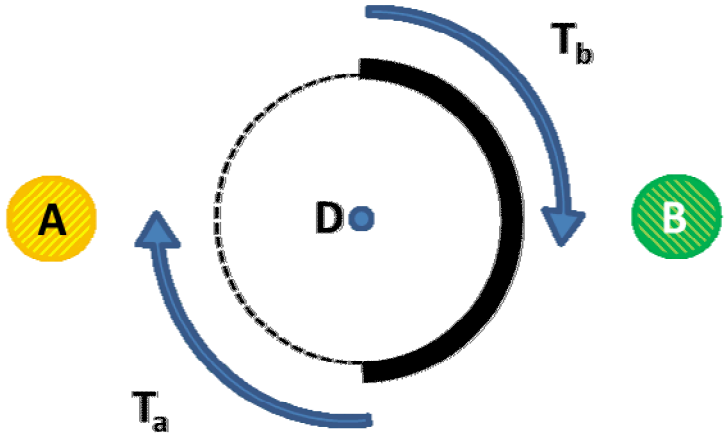
Anti-mask

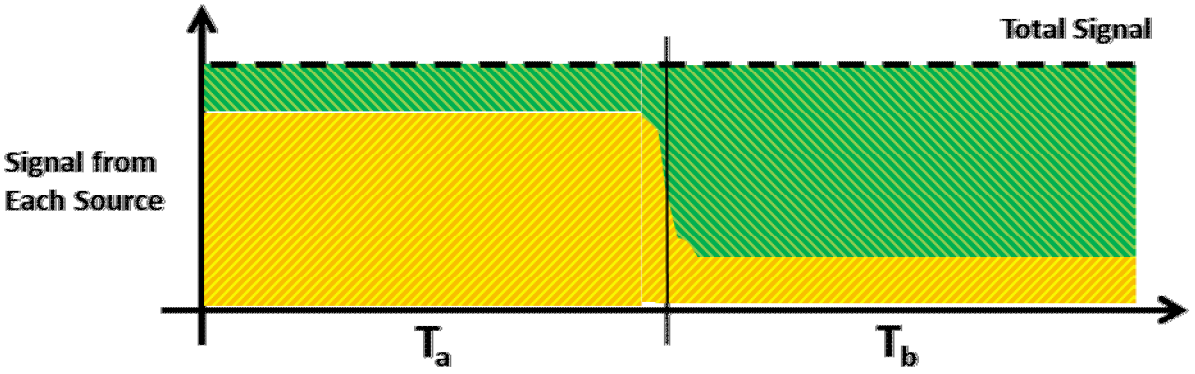
TAI #2



Sandia National Laboratories

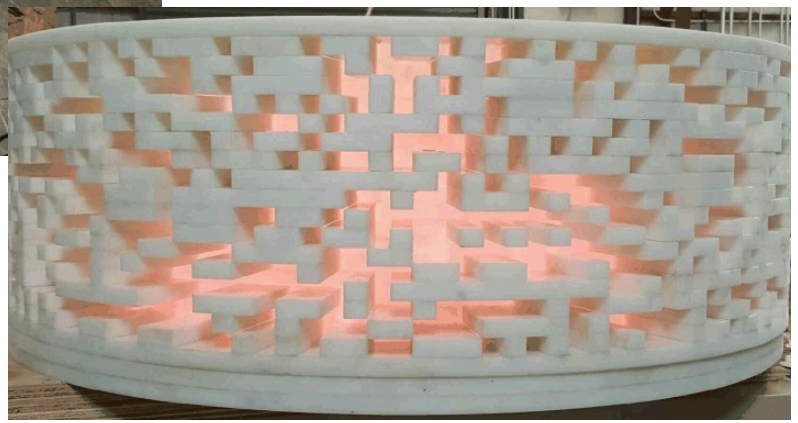
A very simple example





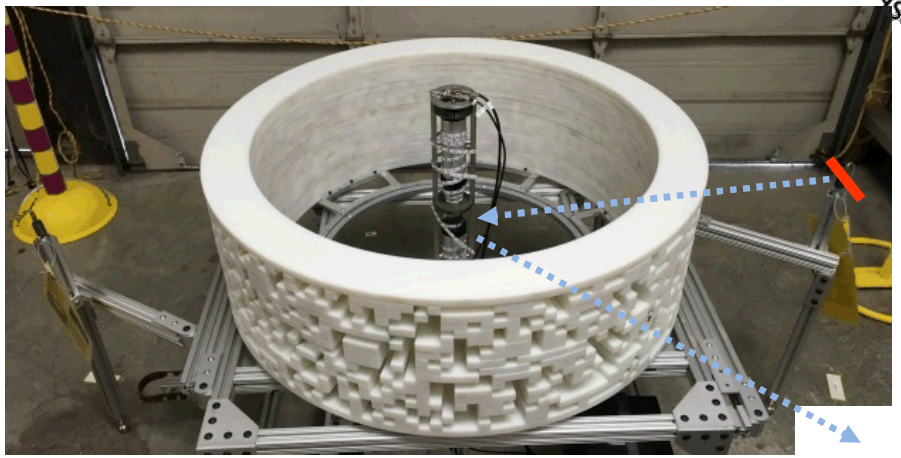
- For example, take a very simple mask: half mask, half aperture.
- The fraction of total count rate coming from A and B is unknown at any given angle.
- In this example, the location (and shape) of the boundary between regions is not revealed.

We've made one!

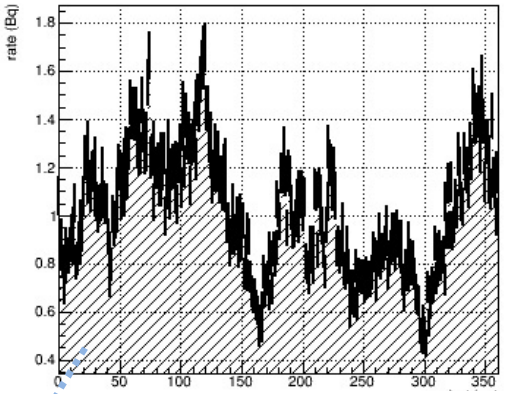


Results – Double point source measurements

Measurement of a double “line” source

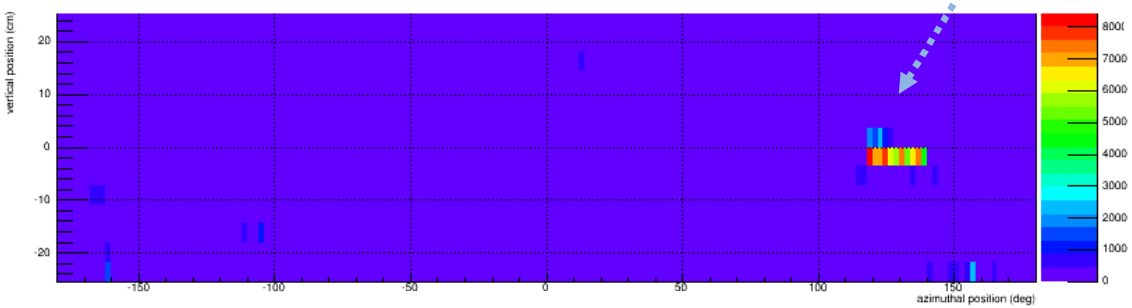


Neutron Rate



Rotation Angle (deg)

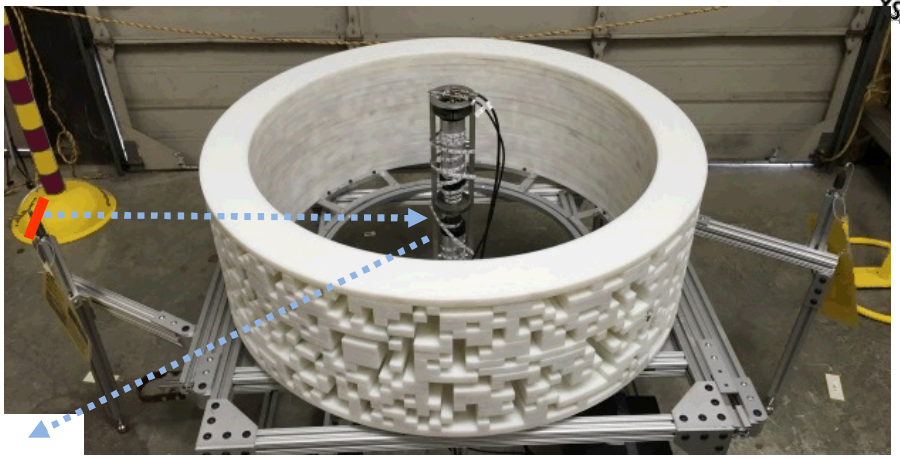
MLEM Reconstruction



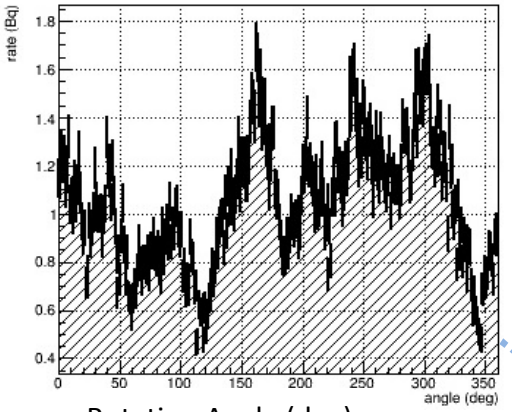
Azimuthal Position (deg)

Results – Double point source measurements

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

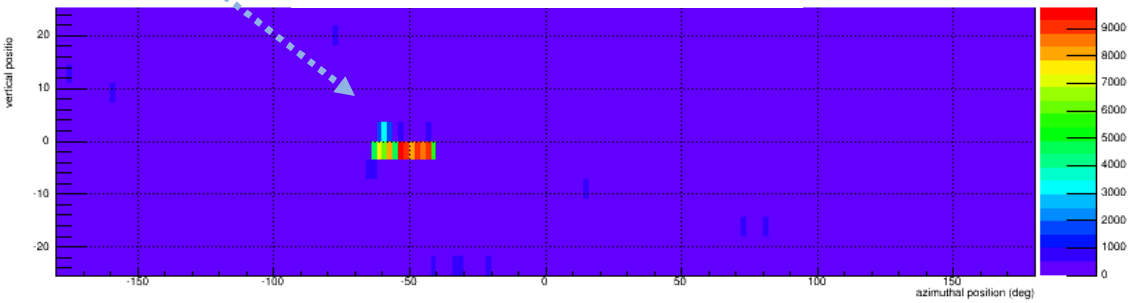


Neutron Rate



Rotation Angle (deg)

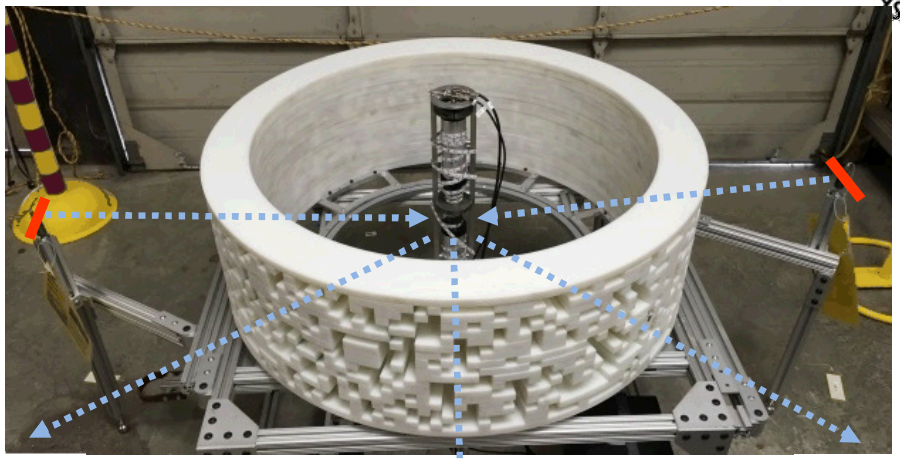
MLEM Reconstruction

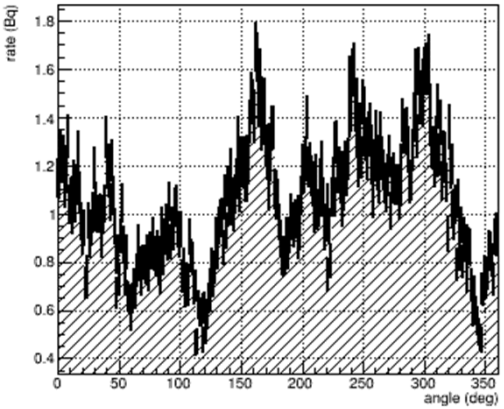


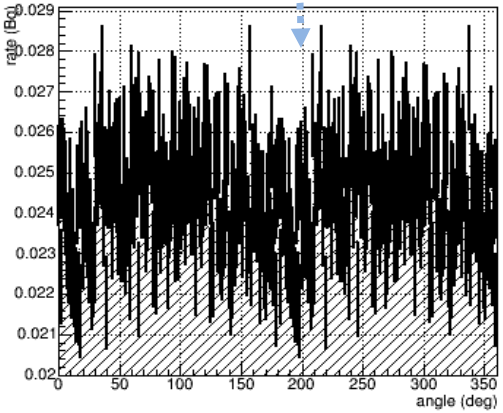
Azimuthal Position (deg)

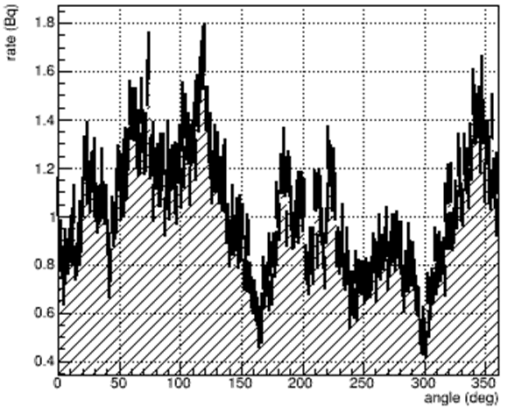
Results – Double point source measurements

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



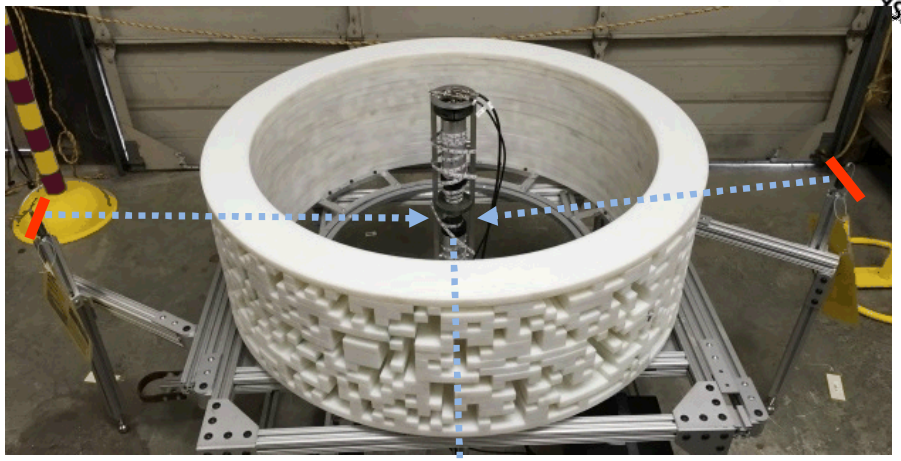






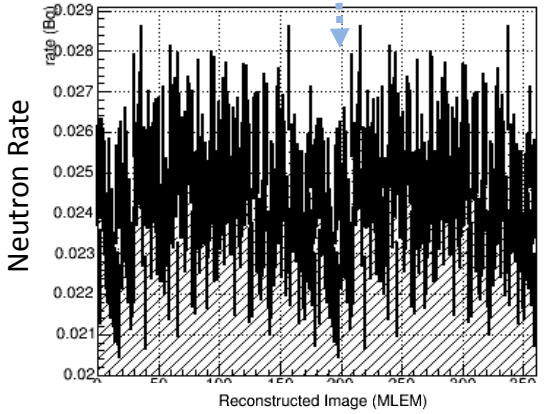
Results – Double point source measurements

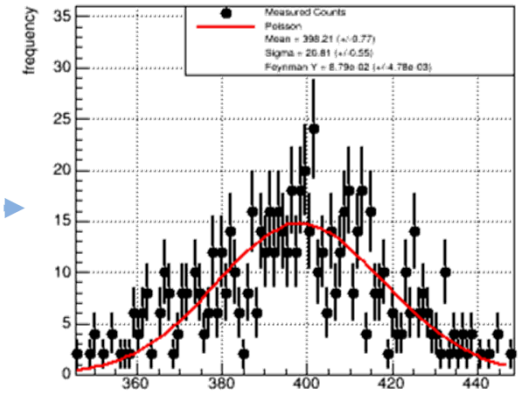
Measurement of a double “line” source (~20 hours total)



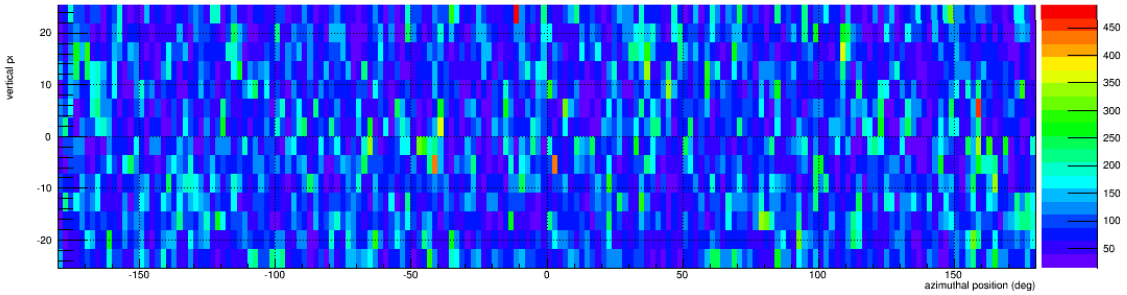
Feynman Y
$= \left(\frac{variance}{mean} - 1\right)$
$= 0.0879 \pm 0.00478$

Count Distribution (Poisson – red curve)





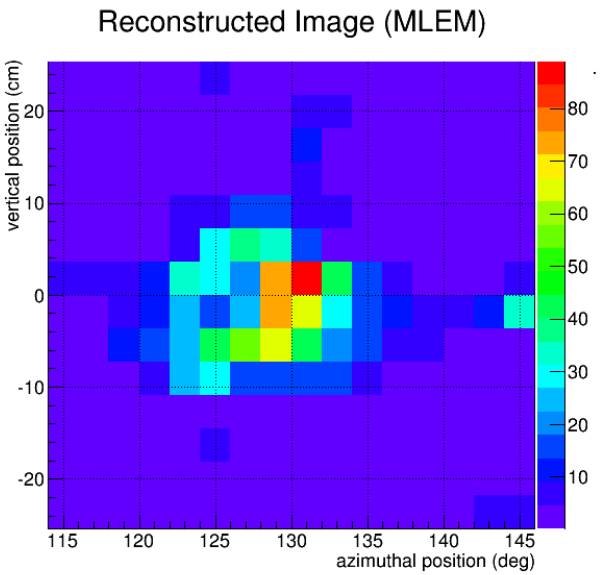
MLEM Reconstruction

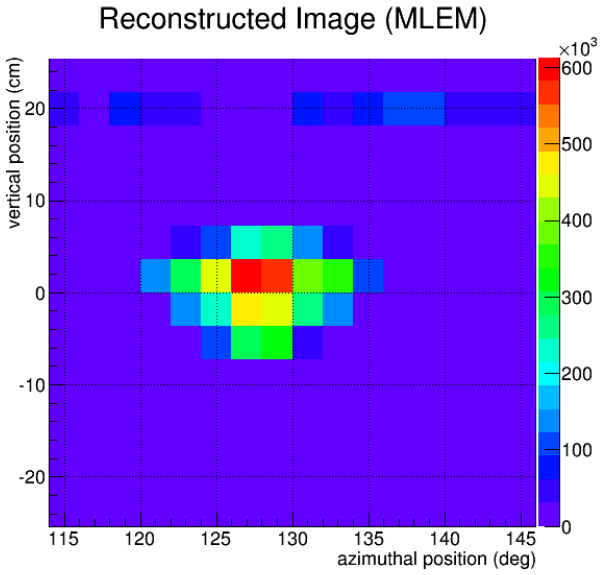


LLNL's PuO_2 Hemispheres

Measurement of plutonium dioxide hemispherical shells at LLNL.

Neutron Image

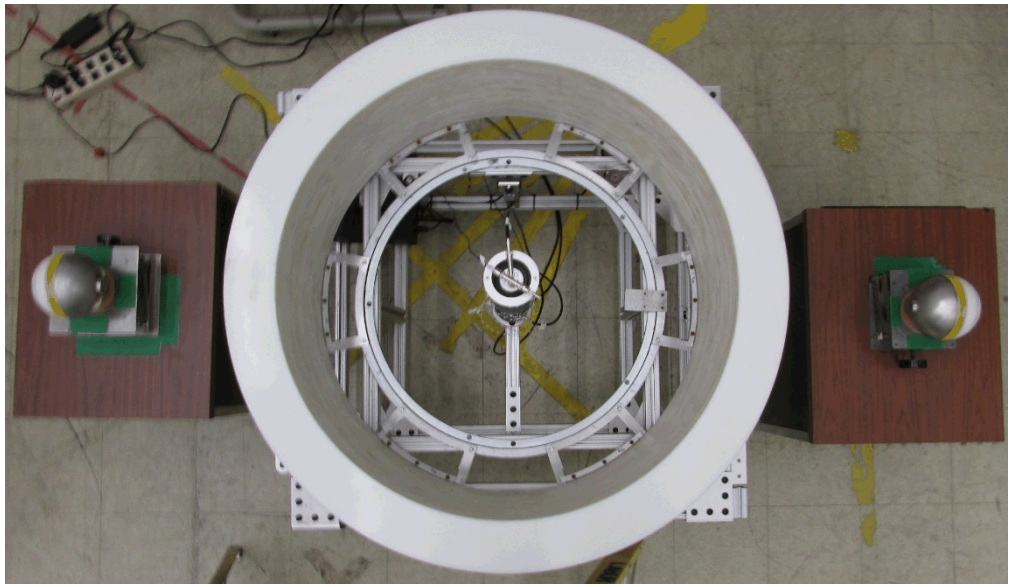




Gamma-ray Image

Sandia National Laboratories

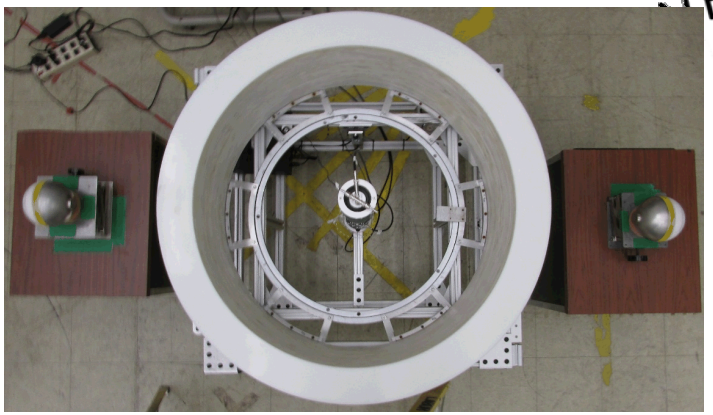
LLNL's PuO_2 Hemisphere comparison measurement



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

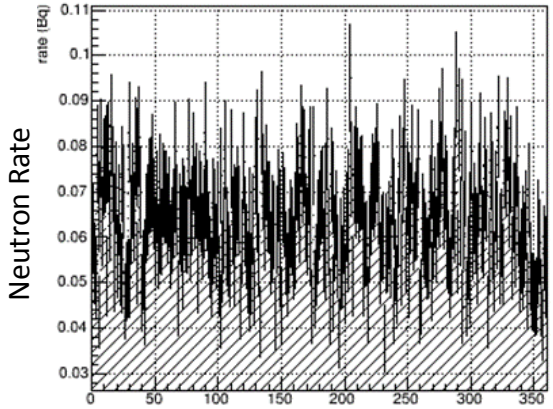
LLNL's PuO_2 Hemi positive measurement

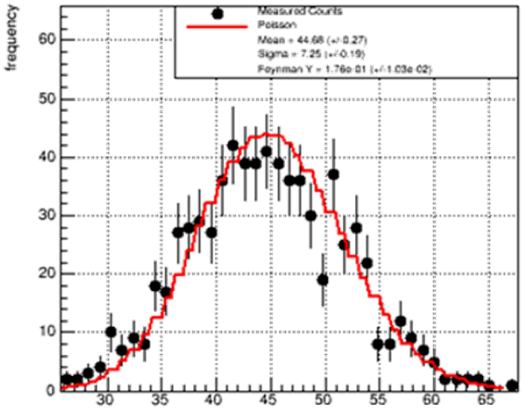
- One hemisphere was placed on each side (180 deg) of CONFIDANTE.
- ~68 hours of data was taken.



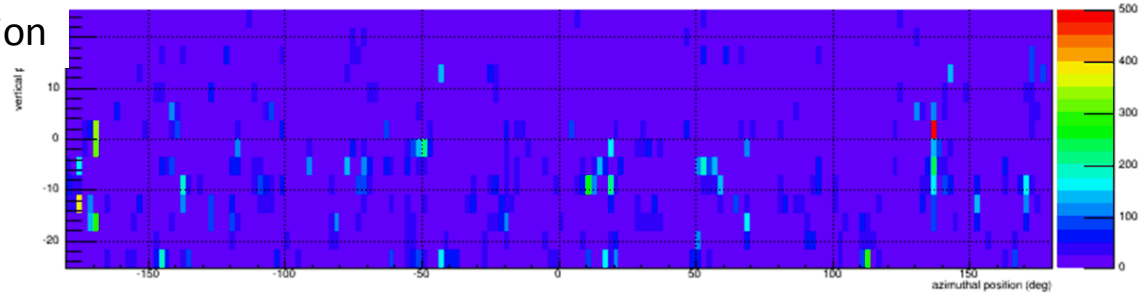
Feynman Y
$= \left(\frac{variance}{mean} - 1\right)$
$= 0.0176 \pm 0.00103$

Count Distribution
(Poisson – red curve)





MLEM
Reconstruction



LLNL's PuO_2 Hemi negative measurement

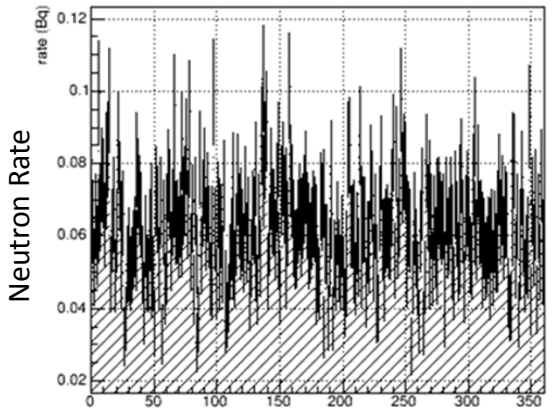
- One hemisphere was placed on each side (180 deg) of CONFIDANTE.
- One was rotated by 90 degrees.
- ~48 hours of data was taken.

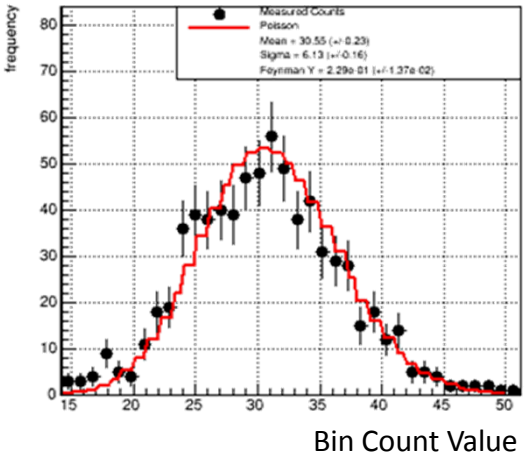
Feynman Y

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

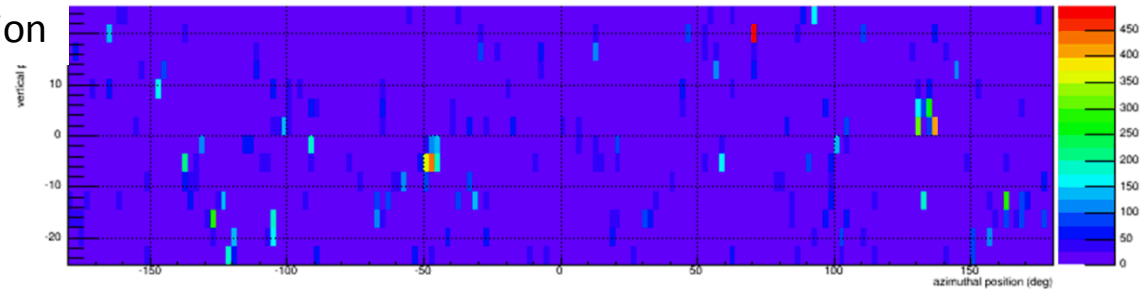
$= 0.229 \pm 0.0137$

Count Distribution (Poisson – red curve)



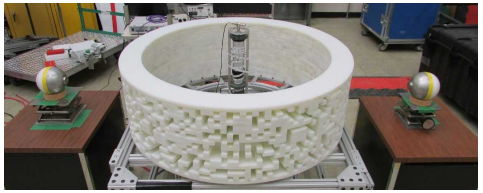


MLEM Reconstruction

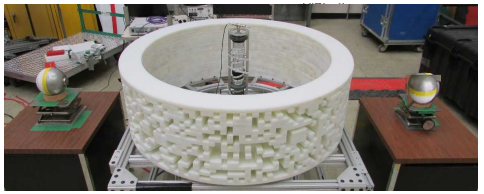


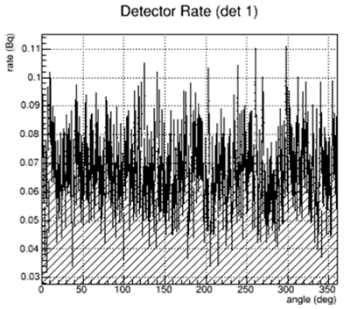
Feynman Y Test Statistic – 10,000 bootstrapped trials

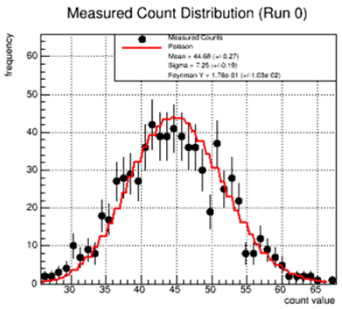
Identical Hemis

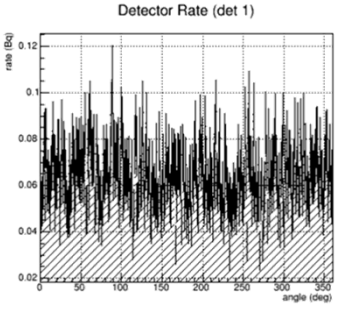


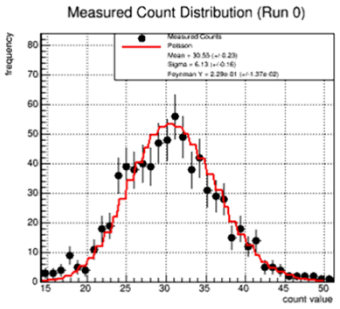
Misaligned Hemis



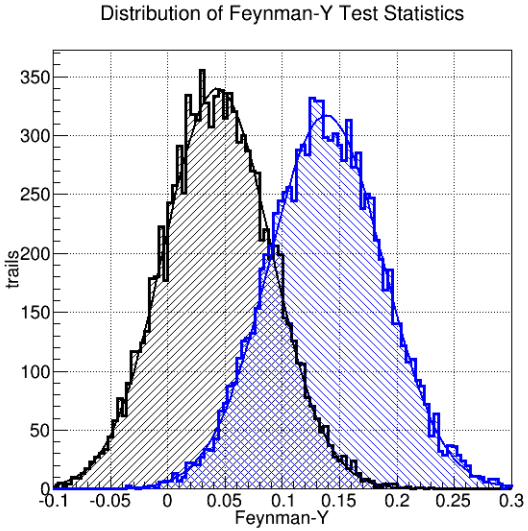








Black – 10,000 bootstrapped trials of two "identical" PuO_2 hemispheres (~48 hours)



Blue – 10,000 trials of two "non-identical PuO_2 hemispheres (~48 hours) (one side rotated by 90 deg.)

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.

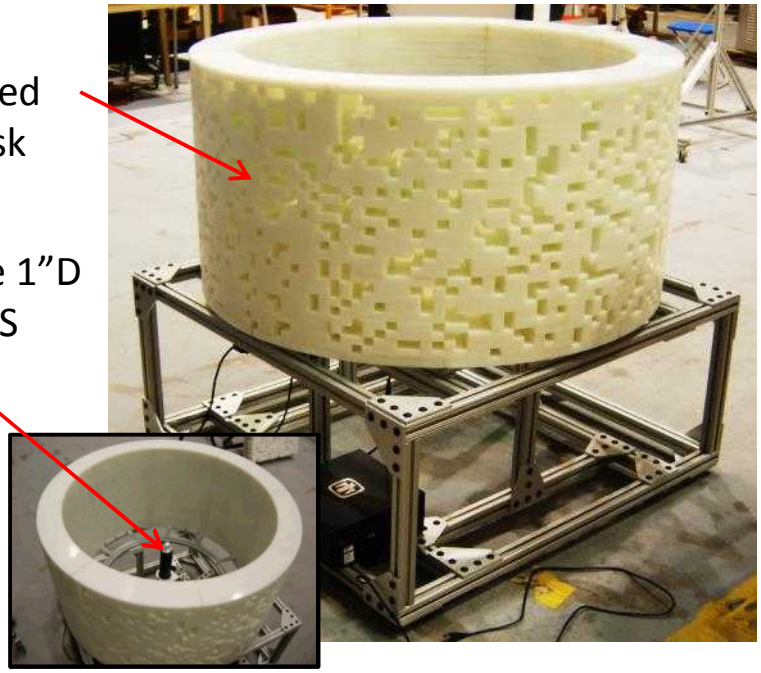
2. Because a NULL (constant rate) is present at all times, the inspecting party might be allowed full access to the measurement and data.

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.

Extra Slides

2D TEI – confirmation measurements?

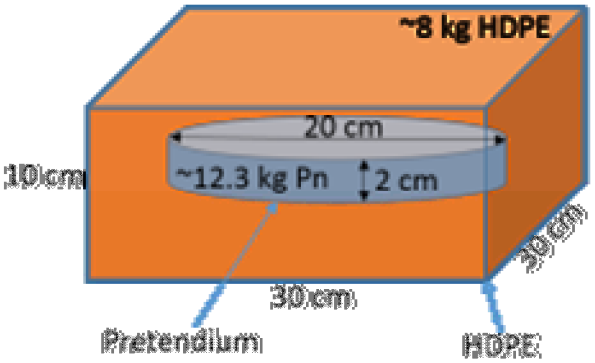


- **TEI is simple**
  1. Only one instrumented channel.
  2. Minimal calibration issues
     a) Information encoded in the relative rate of a single detector.
     b) Absolute gain doesn’t matter.
     c) Gain can drift over time.
  3. Potential real-time analysis
     a) Single data stream.
     b) Events can be processed one at a time and update a test statistic.

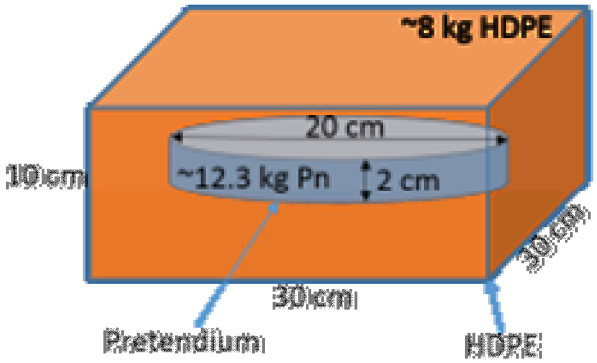
Sandia National Laboratories

Challenge problem

- The inspecting party has or had access to measure item T, which is known to be a valid type 1 treaty accountable TAI through some other mechanism.
- In the course of an inspection, the host presents item X and declares it as a type 1 TAI
- Item X should pass the verification measurement if it is a type 1 TAI, and fail if it is significantly different.



Object T = valid type 1 TAI



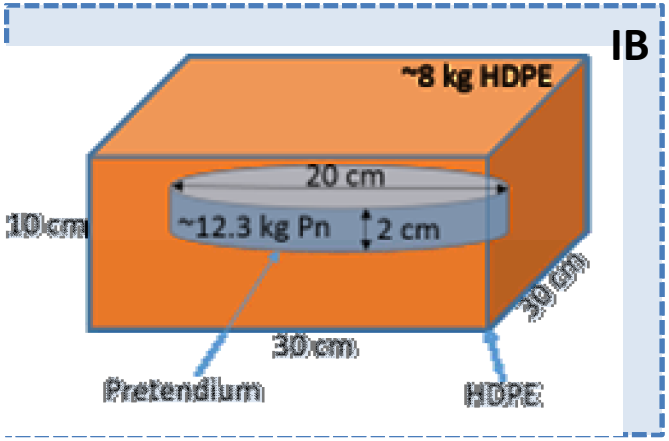
Object X = ?

Sandia National Laboratories

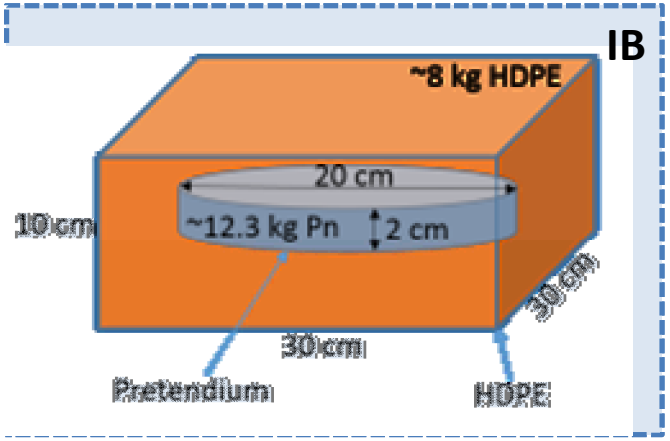
E. Brubaker, "Workshop on Techniques for Protection of Imaging Information: Challenge Problem", SAND2016-4047 O

Challenge problem

- The host must be confident that the inspector has not learned the diameter *d* of the pretendium in item X, or any type 1 TAI



Object T = valid type 1 TAI



Object X = ?

37

Sandia National Laboratories

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