SANDIA REPORT

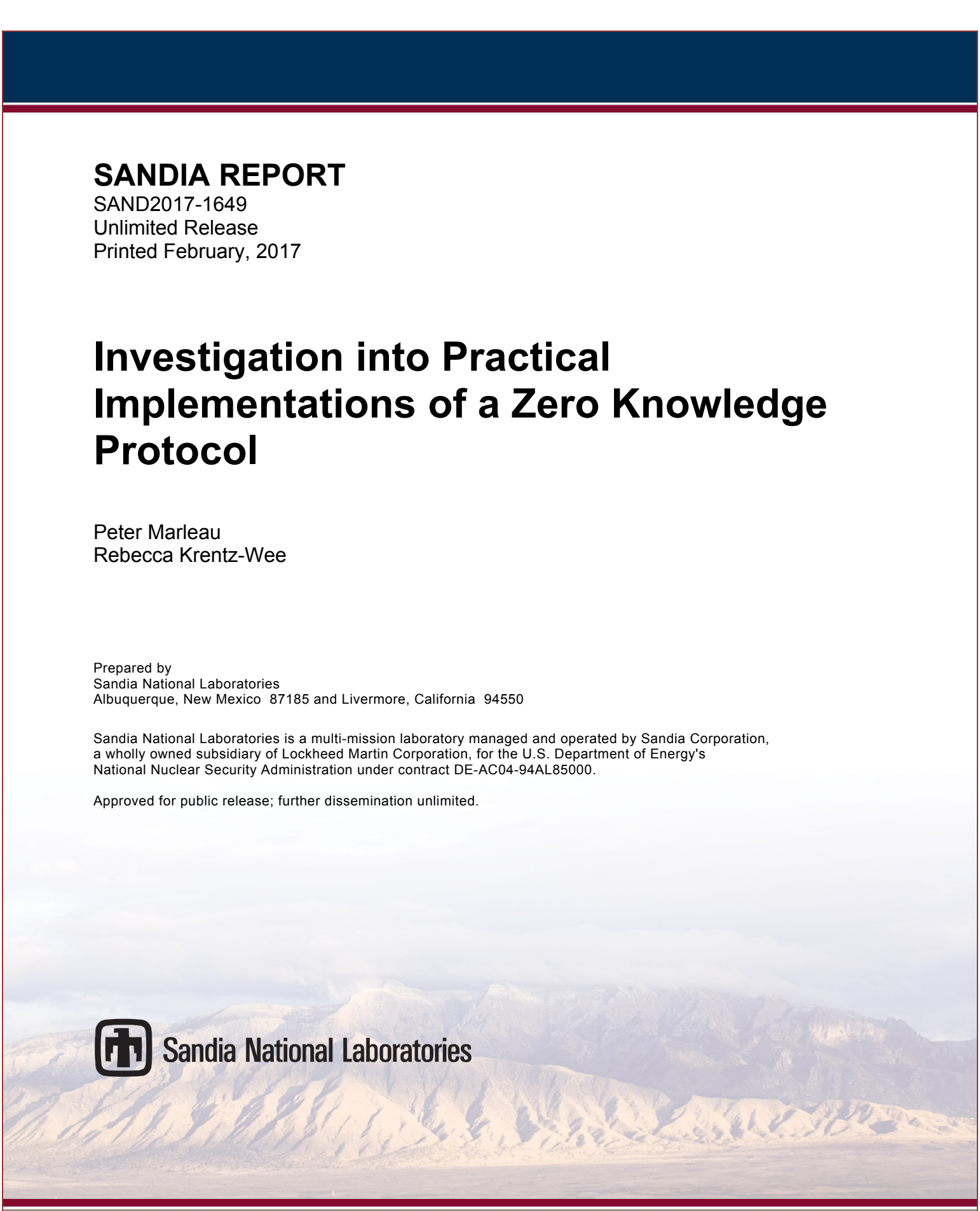
SAND2017-1649
Unlimited Release
Printed February, 2017

Investigation into Practical Implementations of a Zero Knowledge Protocol

Peter Marleau
Rebecca Krentz-Wee

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.



Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/search

SAND2017-1649
Unlimited Release
Printed February, 2017

Investigation into Practical Implementations of a Zero Knowledge Protocol

Peter Marleau and Rebecca Krentz-Wee[1]
Radiation and Nuclear Detection Systems
Sandia National Laboratories
P.O. Box 969
Livermore, California 94551-MS9406

Abstract

In recent years, the concept of Zero Knowledge Protocols (ZKP) as a useful approach to nuclear warhead verification has become increasingly popular. Several implementations of ZKP have been proposed, driving technology development toward proof of concept demonstrations. Whereas proposed implementations seem to fall within the general class of template-based techniques, all physical implementations of ZKPs proposed to date have a complication: once the instrumentation is prepared, it is no longer authenticatable; the instrument physically contains sensitive information. In this work we explore three different concepts that may offer more authenticatable and practical ZKP implementations and evaluate the sensitive information that may be at risk when doing so: sharing a subset of detector counts in a preloaded image (with spatial information removed), real-time image subtraction, and a new concept, CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding (CONFIDANTE). CONFIDANTE promises to offer an almost ideal implementation of ZKP: a positive result is indicated by a constant rate at all times enabling the monitoring party the possibility of full access to the instrument before, during, and after confirmation. A prototype of CONFIDANTE was designed, built, and its performance evaluated in a series of measurements of several objects including a set of plutonium dioxide Hemispheres. Very encouraging results proving feasibility are presented.

[1] Rebecca is currently a graduate student in Nuclear Engineering at UC Berkeley

ACKNOWLEDGMENTS

I would like to thank Vladimir Mozin and Phil Kerr from Lawrence Livermore National Laboratory for their experimental support and Jim Brennan and Dan Throckmorton for the construction of the prototype imaging system.

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 U.S. Department of State.

CONTENTS

FIGURES

TABLES

NOMENCLATURE

ASIC	Application Specific Integrated Circuit
CONFIDANTE	CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding
DOE	Department of Energy
FOM	Figure of Merit
FWHM	Full Width Half Maximum
GW	Golden Warhead
HEU	Highly Enriched Uranium
IB	Information Barrier
LLNL	Lawrence Livermore National Laboratory
MLEM	Maximum Likelihood Expectation Maximization
PDF	Probability Density Function
PMT	Photomultiplier Tube
PSD	Pulse Shape Discrimination
SNL	Sandia National Laboratories
SNM	Special Nuclear Material
TAI	Treaty Accountable Item
TEI	Time-Encoded Imaging
TRADS	Trusted Radiation Attribute Demonstration System
TRIS	Trusted Radiation Identification System
WGPu	Weapons-grade Plutonium
ZKP	Zero Knowledge Protocol

1. INTRODUCTION

Glaser, Barak, and Goldston recently described an approach for nuclear warhead verification based on the cryptographic concept of a zero-knowledge protocol (ZKP) (1). The verification approach includes both procedural elements and a physical implementation. Though ZKP as used in cryptography is a useful model for the arms control verification problem, the direct analogy to arms control breaks down quickly. For example, authentication in zero-knowledge cryptographic protocols is achieved by brute force repetition of the challenge/response procedure; in arms control, repeated measurements are expensive and time-consuming, so a different approach to authentication is needed. In this work, we explore several different concepts that may make ZKP implementations more practical in this sense.

The ZKP methodology fits within the general class of template-based verification techniques. Traditionally, verification technologies have taken one of two approaches toward the confirmation of warhead authenticity: templates or attributes (2). Each of these approaches lend themselves to the application of information barriers; enabling the sequestration of potentially sensitive information in different ways.

Generally, attribute approaches seek to confirm intrinsic characteristics unique to nuclear warheads and/or their components (e.g. isotopic ratio, plutonium mass, etc.). In order to be confirmed, a treaty accountable item (TAI) might have to pass a number of attribute tests by falling within a range of acceptable values. Though the attribute-based approach potentially mitigates the need to develop a sensitive definition of "warhead" (less sensitive ranges of values can be defined), typically sensitive data with a higher degree of detail must be collected in order for the analysis to yield a conclusion, and thus an information barrier must be implemented to protect the sensitive information used in that analysis. Several attribute measurement systems have been developed and demonstrated. A notable example of such a system is the Sandia National Laboratories (SNL) developed Trusted Radiation Attribute Demonstration System (TRADS), which confirms attributes of weapon-grade Plutonium (WGPu) and highly enriched Uranium (HEU) using a high-purity germanium detector (3). TRADS was developed with special care to provide an authenticatable and certifiable acquisition and analysis system using trusted processors.

Template approaches utilize data taken from a trusted reference object to compare to measurements of declared items, confirming that they are the same item or class of item. This approach also skirts the issue of developing a sensitive definition of "warhead", but requires that a reference object be pre-authenticated by some other means. In addition, the template itself is likely to contain sensitive information and thus needs to be protected by an information barrier. An example of a template-based implementation is SNL's Trusted Radiation Identification System (TRIS) (4). TRIS included a physical and software security architecture that enabled it to confirm the authenticity of TAIs without revealing sensitive information.

Several experts at Sandia National Laboratories, including TRIS and TRADS developers, recently presented an analysis of the benefits and challenges of Zero Knowledge Protocols over more traditional warhead verification approaches (5) (6). It was generally agreed that the physical implementations that have recently been proposed (such as that found in (1)) fall within

the class of template-based techniques. However unlike TRIS in which the sensitive template is kept sequestered, in the proposed ZKP approaches, the template is "preloaded" into the physical measurement system. This is problematic for two reasons:

1. The "preloaded" template is of one-time use. The detector is prepared in such a way that a measurement should produce a flat field "NULL" result if the object matches the reference. Once a measurement is made, the preloaded template is effectively destroyed. It is therefore impossible to keep chain of custody on the "template" which would normally lend credibility to its authenticity.
2. Once the "template" is preloaded, the instrument itself contains sensitive information and may be off limits to the monitoring party. It could therefore be detrimental to the authentication of the measurement process. If authentication steps cannot be identified, then host party must preload and use the instrumentation entirely behind an information barrier.

In this work we investigate whether practical, more authenticatable implementations of a Zero Knowledge Protocol may be developed in three approaches:

1. Building upon the concept of last-minute selections of equipment and items to be inspected in the ZKP approach, we explore the possibility of whether a subset of the counts in a preload might be shared with the inspecting party. This approach was explored with a simulation of an evaluation object. Counts, stripped of their spatial location, were analyzed statistically to determine what information might be retrieved regarding the original source distribution. The results are presented in Section 2.
2. We investigate a concept by which the images of two objects might be subtracted in real time. As a pixel count from one object is registered in one imager, it is added to the image, while the pixel count from another object in a second imager is subtracted. This opens the possibility of eliminating the need for a detector preload by effectively loading the inverse image using a second detector. This approach was explored in Monte Carlo simulations and the resulting images were statistically analyzed to evaluate whether sensitive information might still be learned from the subtracted count distributions. Results are presented in Section 3.
3. Designing a new implementation that does not require preloading of the instrument, rather it creates the complement image and adds it to the measured image during the measurement causing a NULL positive condition to be present within the instrument at all times. Therefore, the monitoring party could be allowed full access to the instrument and its data at all times, even to the point of conducting the measurement themselves. This concept, dubbed CONFIDANTE (CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding), was tested both in simulations and in the laboratory with a prototype imaging system. Results from Monte Carlo simulations laboratory tests are presented in Section 4.

2. SHARING OF PRELOADED NEUTRON DETECTOR COUNTS

Because the host generally owns the preparation and use of measurement equipment and even the data collected, the additional role of inspector choice can contribute significantly to confidence in a measurement. For instance, within the context of either active fast neutron transmission images as presented in (1) or passive fast neutron images, if the inspector were permitted to independently measure the count rates in some or all of the imaging detector pixels at various stages of the inspection, confidence in the authenticity of both the equipment and measurement would be gained.

It is almost certain that the spatial orientation of count rates contains sensitive information. However, it is possible that the distribution of count values might be acceptably less sensitive. The count values could be shared at several stages during the confirmation process:

1. After a measurement – As described in the ZKP approach, the measurement instrument is preloaded with the inverse of the expected image such that a positive result gives a flat field image with only statistical fluctuations. In theory, the detector count rates (or detectors themselves) could be shared with the inspector. However, we have identified a possible weakness with this approach. Misalignment of the instrument and/or inaccurate dose delivered (dwell time or neutron output) could result in deviations from flat field. Again, the spatial distribution of counts will reveal some features of the template; however, the randomized distribution of counts might not.

2. A random sample of pixels before a measurement – Even if a random sample of pixels out of a preloaded inverse image were allowed to be removed and measured, confidence in the authentication of the equipment would be gained. Because all of the sensitive information is encoded in this preload, even a subset of these pixels could be sensitive, especially if their location within the image were known.

3. Before a measurement – If all of the spatial information were removed (e.g. – all of the detectors were dumped into a bucket first), then what sensitive information remains in the full count distribution of the preloaded inverse image?

Through inspection of the detectors and their content before and/or after a verification measurement takes place, confidence could be gained that the equipment is functional. By further adding tamper indicating tags and seals on the detectors, confidence could also be gained that the measurement took place.

We have investigated what sensitive information might be present in the count rates within passive emission images in the third category. Count distribution information obtained in the first two categories can lead to the reconstruction of the full count distribution after multiple measurements. Therefore, we have begun with this worst case scenario.

2.1. Monte Carlo Simulation

In order to evaluate what information might be present in the distribution of pixel counts in an image, we designed a passive neutron imaging Monte Carlo simulation. The passive imager, shown in Figure 1, comprises a 10 cm thick High Density Polyethylene (HDPE) mask with a single 1 centimeter diameter hexagonal pinhole aperture and a 4x4 array of pixelated block detectors (10x10 1 cm pixels each) modeled after the ORNL/SNL Neutron Coded Aperture Imager (7) for the image plane. For all simulations a mask plane to image plane (center to face) separation of 1 meter and a mask plane to source plane (center to center) separation of 2.54 meters was used. An example point spread function (point source forward projected onto the image plane) is shown in Figure 2.

A pinhole imager was chosen for this study because the passive emission images on the image plane are a reasonable proxy for a transmission radiograph onto an image plane. The obvious difference being that a radiograph images the attenuation through materials exhibiting dark regions, whereas an emission image exhibits a brighter region in the location of emitting materials. In this way, a passive emission pinhole image is representative of the type of pattern that might need to be preloaded into a detector array in reference (1).

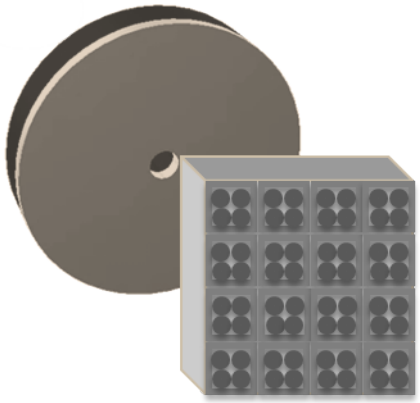


Figure 1 – Illustration of the passive coded aperture imager used in this simulation.

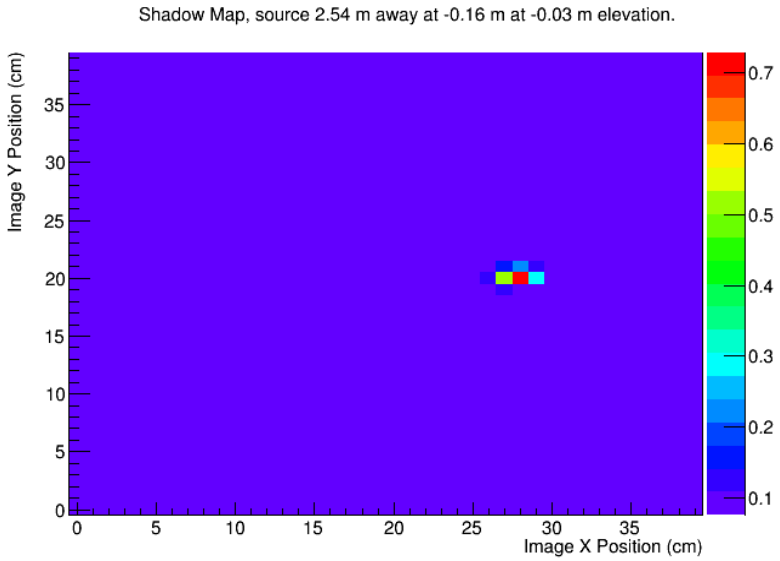


Figure 2 – The passive coded aperture point source relative response on its 40x40 pixel array.

2.2. Results

An evaluation object source distribution in the shape of a hollow rectangle, shown in Figure 3 (left), was used. The ratio of counts in the signal (rectangular) region to the sum of all background regions is 100 to 1. The background was distributed uniformly across the entire field of view of the imager. The source pixel count distribution used as input to a Monte Carlo simulation is shown in Figure 3 (right).

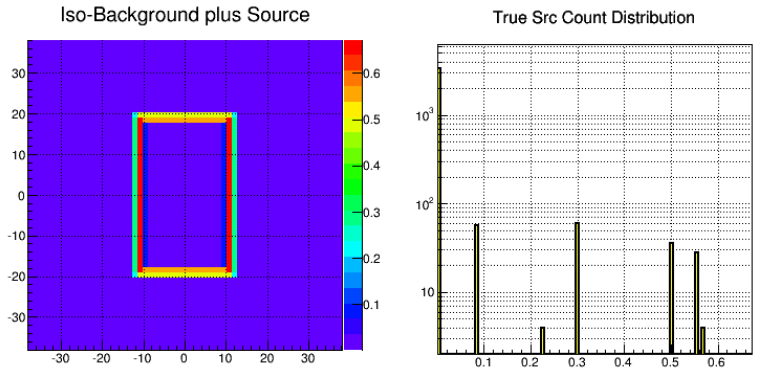


Figure 3 – (Left) An image of the evaluation object source distribution used as an input to the simulations. (Right) A histogram of the evaluation object's relative pixel count distribution in its image.

In this study, 1e7 detected counts were thrown from this source distribution and forward projected through the pinhole imager. An example distribution of counts in the detector image plane is shown in Figure 4 (left). Upon close inspection, it can be seen that the ratio of source region to background region counts now greatly exceeds 100 to 1. This is caused by fast neutrons transmitting through the mask unimpeded. This lack of mask opacity effectively reduces the signal to background ratio to 0.167.

Even so, there remains enough signal to noise that a simple threshold applied at a value of 6400 counts easily removes all of the background pixels as shown in Figure 4 (center).

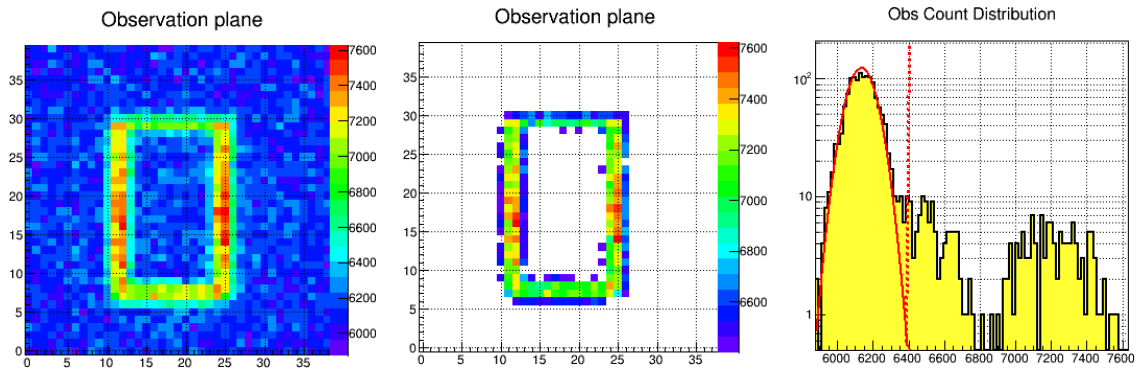


Figure 4 – (Left) A histogram of the count distribution on the 40x40 pixels of the coded aperture's image plane. (Center) The same histogram with any pixel having fewer than 6400 counts removed. (Right) A histogram of the pixel count distribution in the image on the left. The red curve is the expected distribution for random Poisson noise and the red line at 6400 is the threshold for creating the center image.

This can be seen more easily in Figure 4 (right), the histogram of the pixel count values found in Figure 4 (left). This would be the distribution of counts found in detector pixels if the spatial location of each pixel were ignored and is analogous to the count distribution that might be preloaded into a detector pixel array in the ZKP implementation described in (1).

The aforementioned threshold of 6400 counts is indicated by the vertical red dotted line. The distribution of counts that would be expected from a random Poisson noise source with a mean of 6180 is also indicated by the red curve. We should emphasize that this is not a fit, but rather the calculated expectation for a randomly distributed source. With full knowledge of the opacity of the mask, this distribution is entirely predictable.

Because all pixels contributing to the source regions of the image have values to the right of this line, we can immediately estimate the size of the source distribution as being ~230 pixels, the number of entries with a value greater than 6400. Further, with knowledge of the mask opacity, we also have an estimate of the total counts that can be attributed to the source.

Therefore, it is possible to estimate both the total source activity and angular size of the object. It is not a stretch to assume that even these estimates tread on sensitive information that a host party may want to protect. With some knowledge about the approximate shape of the object, it may also be possible to perform a dictionary attack on this distribution, enabling a monitoring party (should they be allowed access to this count distribution) to narrow in on a range of shape models. Because this source distribution can be estimated through multiple trials even if only a sub-set of the pixel values are shared, we cannot recommend this as a means of improving measurement authentication.

3. REAL-TIME PIXEL WEIGHTING

As was learned in Section 2, the pixel count values should be protected at all times prior to the completion of a measurement; at which time the NULL positive condition will have been satisfied. In order to gain access to the instrument and/or detector counts before or during the measurement process, the NULL positive condition should always be present. We have investigated two concepts by which this might be achieved: Real-time Pixel Weighting and CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding. The latter is explored in Section 4.

Inspired by methods that have been recently proposed as information barriers that implement window weighting schemes on gamma-ray spectral measurements in real time, we first explore a concept by which two imagers, operated in tandem, measure two objects simultaneously. If the two objects being measured are identical in radiation emissions and spatial distribution of materials, and the two imagers are identical in response, then the subtraction of the detected counts in each pixel should have a mean of zero.

This is illustrated in Figure 5; two independent measurements of two identical objects (left and center) produce the NULL image on the right, with mean count value of zero (the absolute value of count differences is shown in the figure). However, if the two objects are not identical in spatial extent as illustrated in Figure 6, the resulting image is the difference set of the two objects. The host party then has incentive not to attempt a spoof as the difference set is likely to reveal some sensitive information regarding the spatial extent of the trusted reference object (Golden Warhead).

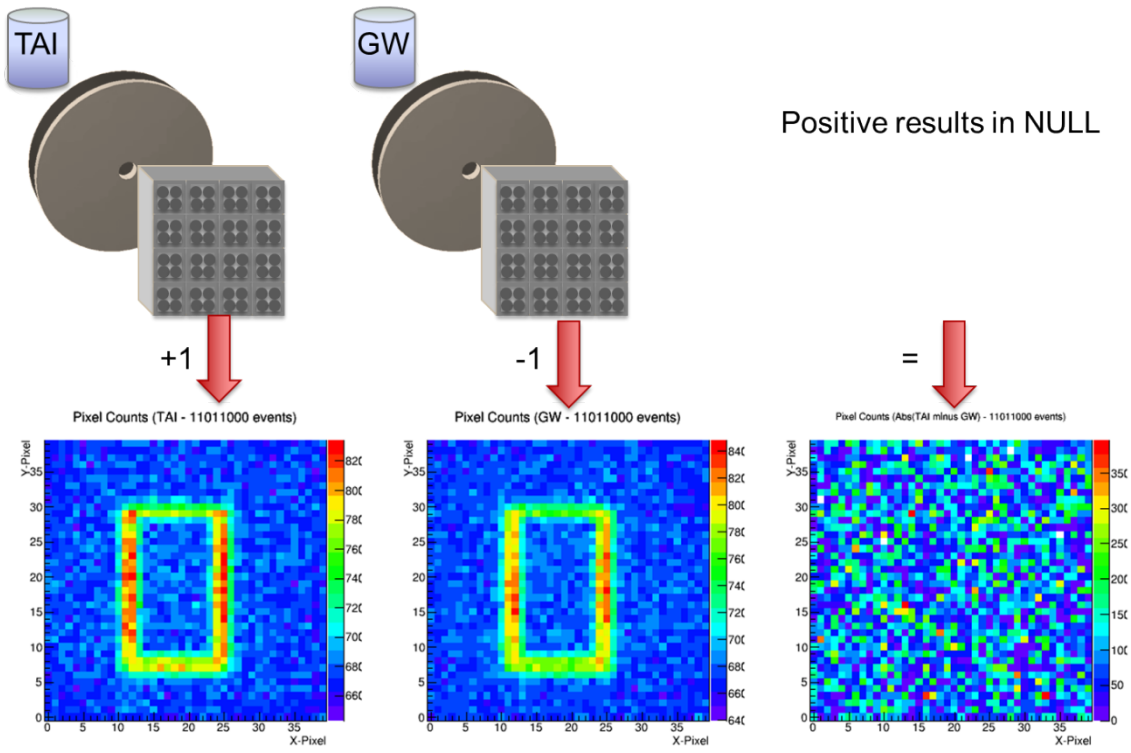


Figure 5 – Illustration of the real-time pixel weighting concept. The pixel count distribution from imager number one (left) is added to the pixel count distribution of imager two, that has a weight of negative 1. If objects 1 (a TAI) and 2 (a trusted reference "Golden Warhead") are identical, then the sum will be consistent with Poisson noise.

Leaving aside the extreme difficulty in maintaining two imaging systems with identical response functions, let alone a single system with calibrated pixel responses, this concept seems to have merit. However, we must investigate further the statistical fluctuations in the difference set. It is true that the difference of two count distributions with the same mean will have a mean of zero, but the variance of the difference set distribution will be proportional to the sum of the variances of the original distributions (assuming normal counting statistics). Therefore, there is residual information regarding the original count distributions in the variance of a difference set.

With multiple positive trials, one could begin to estimate the variance of the distribution for each pixel and eventually reconstruct the original images. For example, in order to discriminate the standard deviation of counts in a pixel in the source region with mean counts N from the standard deviation of counts in a pixel in the background region with mean counts εN, where ε is the effective transmission coefficient for the mask, one might require that their difference be larger than some fraction, k, of the standard deviation of background counts:

Equation 1 – Condition for detecting a difference in the standard deviation of two regions.

$$\sqrt{2N} - \sqrt{2\varepsilon N} > k\sqrt{2\varepsilon N} \rightarrow \varepsilon < \frac{1}{(k+1)^2}$$

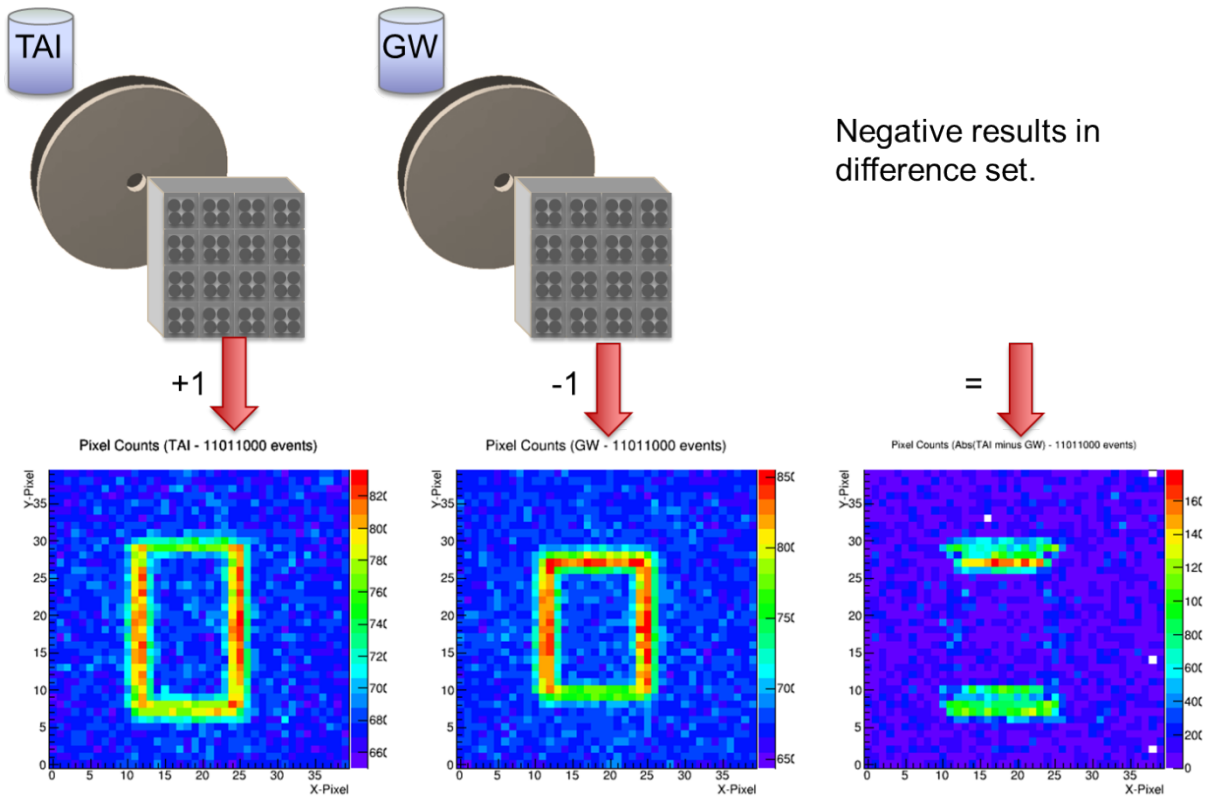


Figure 6 - Illustration of the real-time pixel weighting concept. The pixel count distribution from imager number one (left) is added to the pixel count distribution of imager two, that has a weight of negative 1. If objects 1 (a TAI) and 2 (a trusted reference "Golden Warhead") are not identical, then the sum will not be consistent with Poisson noise and the resulting image will be the difference map of the two objects.

It is worth noting at this point that the mean number of counts, N, has dropped out of Equation 1. The ability to discriminate between the standard deviation of difference count values in two regions depends only on the effective transmission coefficient of the mask, whereas the ability to discriminate between count values of two pixels in an image depends on the square root of the number of counts:

Equation 2 - Condition for detecting a difference in the mean counts in two regions.

$$N - \varepsilon N > \sigma\sqrt{\varepsilon N} \;\rightarrow\; \sigma^2 > \frac{N(1-\varepsilon)^2}{\varepsilon}$$

Where σ is a threshold on the standard deviation of background counts demanded for positive detection of a deviation. For example, in this test case $\varepsilon = 0.8$, $k = 0.11$, and $N = 820/pixel$. So the significance of counts in a single pixel in the signal region over the background region is $\sigma = 6.2$.

On the surface, this is an encouraging result in that the image quality of any one measurement can be improved with the square root of dwell time (being linearly proportional to N), but the ability to discriminate the difference in two images based on the standard deviation of their difference counts depends only on a property of the imaging system; namely, how poorly does the mask block radiation. It may be possible to construct a mask with a large effective

transmission coefficient (i.e. poor mask opacity) such that it is not possible to estimate N from the variance of measured counts in the difference set even after many trials. However, this will drive the measurement to longer and longer dwell times.

As another example, the simulated measurements shown in Figure 5 and Figure 6 had 10^7 detected counts in them. The Neutron Coded Aperture Imaging System (7) would take several days of dwell time to achieve this with a 10^5 n/s neutron source. A pinhole imager could take 100s of times longer than that.

Even so, estimating the standard deviation to within k = 0.11 with a confidence of 95% (2 sigma) requires only 200 samples. This is in fact roughly how many pixels that are in the source regions of Figure 5 (left and center). To illustrate this, if we plot the count difference values in the background and source regions of Figure 5 (right) separately (shown in Figure 7), then fit them with Gaussian functions, we can accurately estimate their standard deviations with a fit error of ~10%. This is just within the difference of standard deviations of these two distributions.

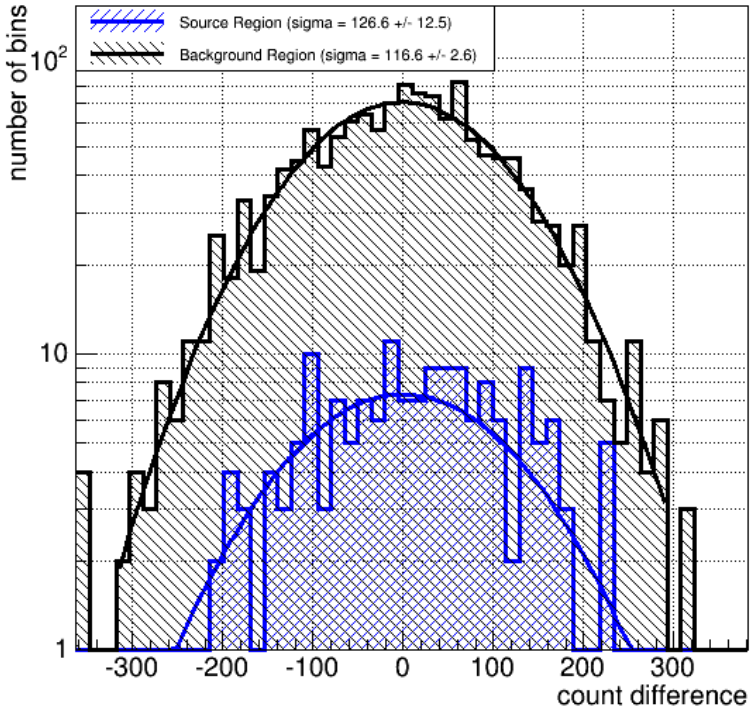


Figure 7 – The distribution of pixel weighted sums in the background (black) and source (blue) regions of the images. The solid curves are a Gaussian fit to the distributions with widths (in sigma) reported in the text box above.

Though the concept of real-time pixel weighting and summing of two images has several positive features, such as having a NULL-positive condition at all times[2], no preloaded

[2] Arguably this is not true since the variance of counts in different regions do contain information about the image

instrumentation, and no reference templates[3], it also has several challenging drawbacks. Ideally, the measurement instrumentation will exhibit counting noise and only counting noise at all times. However, this concept does have an information leak through the variance of count values in the difference set. Though the leak can be reduced, it cannot be eliminated while maintaining reasonable measurement times. Furthermore, calibrating a single pixelated system for uniformity of response is a difficult enough task; cross calibrating two complicated pixelated imaging systems to have identical responses could be considered an epic undertaking. We therefore cannot recommend that this concept be used to improve the authentication of ZKP implementations.

count values. Additionally, each time the difference set is viewed this counts as another sample. Therefore, variance in multiple snapshots of a measurement will allow one to estimate the count values even more quickly.

[3] Because the reference measurement is made alongside the confirmation measurement.

4. CONFIRMATION USING A FAST-NEUTRON IMAGING DETECTOR WITH ANTI-IMAGE NULL-POSITIVE TIME ENCODING

In Section 3, we presented the concept of making simultaneous measurements of two treaty accountable items (TAIs) as a means of effectively eliminating the need for a reference template or preloaded instrument. In this way, one of the objects itself acts as the reference and the confirmation measurement compares images in real-time. As we have seen, an ideal ZKP measurement system will make this comparison in a way such that a positive result is indicated by only Poisson counting noise at all times.

Here we present an authenticatable verification measurement concept using two-dimensional time-encoded imaging (2D-TEI) that we have dubbed CONFIDANTE (CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding). 2D-TEI consists of a single (or few) detector pixel(s) surrounded by a rotating cylindrical coded mask. High resolution fast neutron 2D-TEI has recently been demonstrated in proof of concept measurements of extended fission sources (8). Here we demonstrate that a 2D-TEI with a properly designed coded mask will exhibit an unmodulated detection rate if and only if two objects placed on opposing sides of the system are identical in geometry and activity. Because a positive is indicated by pure counting noise in a single detector pixel and no sensitive information must be "pre-loaded", this concept may prove to be an ideal candidate technology for ZKP confirmation measurements.

4.1. Time-Encoded Imaging

Recently, the feasibility of two-dimensional time-encoded imaging (2D-TEI) as a viable option for high resolution imaging of extended neutron-emitting sources has been demonstrated. As shown in Figure 8, 2D-TEI consists of a single (or few) detector pixel(s) surrounded by a rotating cylindrical coded mask. The mask pattern that is normally projected onto a position-sensitive, highly-pixelated detector in traditional coded-aperture imaging becomes time-encoded in the modulated rate of the pixel(s) as a function of mask rotation angle. Reference (8) provides a more detailed description of the proof-of-concept system and the imaging concept.

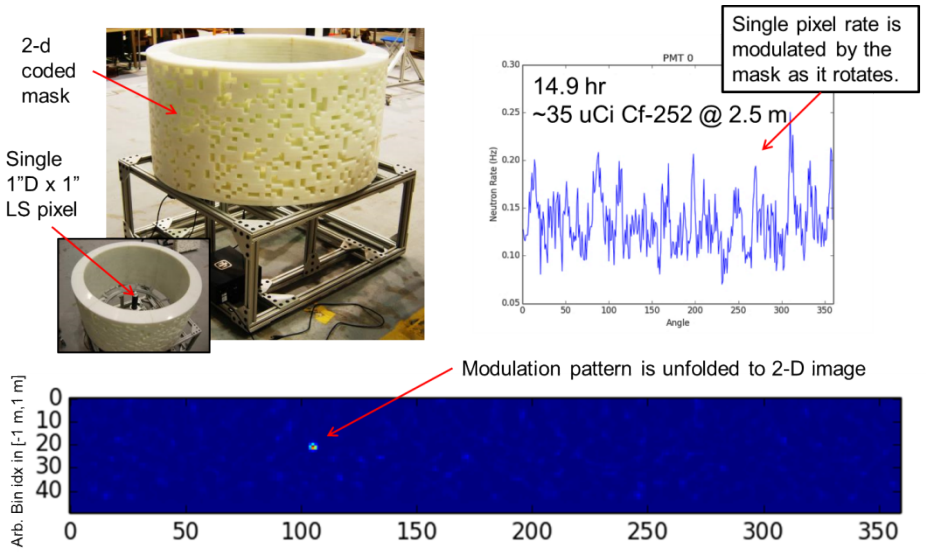


Figure 8 – The proof-of-concept time-encoded imager (upper left) consists of a single 1" diameter by 1" deep liquid scintillator cell surrounded by a rotating cylindrical high density polyethylene coded mask. The modulated neutron detection rate (upper right) has the entire 2-dimensional field of view encoded in its pattern. The Maximum Likelihood Expectation Maximization (MLEM) unfolded image is shown (bottom).

4.2. CONFIDANTE

CONFIDANTE is a confirmation measurement concept based on two-dimensional time-encoded imaging that may remove the need for any explicit information barrier. Sensitive information is physically eliminated at the detector by virtue of the superposition of two radiation fields (one from each of two TAIs) with opposite modulation patterns. The key requirement, therefore, is to use a cylindrical mask pattern in which one 180^{o} half is the anti-mask of the other half; where anti-mask is defined as the replacement of all mask elements to apertures and vice versa.

4.2.1. Concept

The concept in its simplest form is illustrated in Figure 9. At the top of Figure 9 a top view of the mask surrounding detector D is shown. Objects A and B, identical in activity and spatial distribution, are positioned on opposite sides of D. In this example, the mask is entirely closed on one half and open (aperture) on the other. This is the lowest number of mask and aperture elements possible with the property that one half is the anti-mask of the other.

At the bottom of Figure 9 we illustrate a hypothetical detection rate as a function of rotation angle. When the aperture is facing object A (through region T_a), the total rate is composed of a higher fraction of A than B. There may still be some fraction of signal from B because the mask is not perfectly opaque. We see that as the mask rotates through the boundary between T_a (where the aperture faces A) and T_b (where the aperture faces B), the relative fraction of signal from A and B swap. However, the total rate remains unaffected and therefore there is no indication of where this transition occurs, even if monitored. Effectively, the pattern projected from A onto D is the complement of the pattern projected from B onto D at all rotation angles.

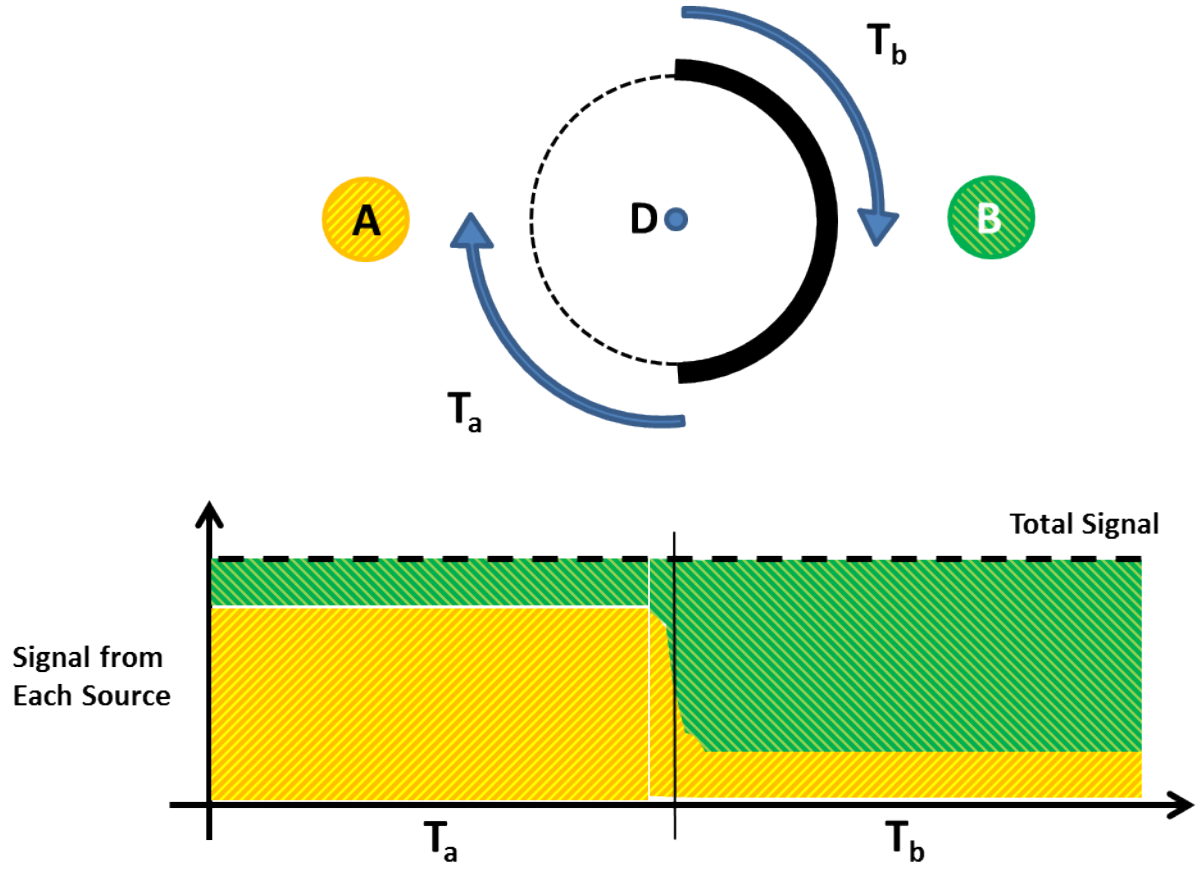


Figure 9 – (Top) Top view of an illustration of the proposed concept using the simplest example of a mask designed with one half as the anti-mask of the other. (Bottom) If A and B are identical, then the sum of signals (y-axis) will be constant as a function of rotation angle (x-axis) even though the contributions from A and B vary.

In this illustration, we show a transition whose shape depends on the volumetric distribution of neutron emitting material within A and B, but the sum of signals from A and B are always equal. This property remains true regardless of how complicated the sources' spatial distribution may be. In order to demonstrate this, we have constructed a toy model as an example. Figure 12 through Figure 16 display a progression of these results.

4.2.2. Proof-of-concept prototype imaging system design

We first designed a two-dimensional mask with the same geometric properties (mask radius, aperture sizes, mask thickness, etc.) as that used in the physical demonstration system described in (8). The mask comprises a stack of nineteen 1.9 cm thick sheets of High Density Polyethylene (HDPE) that were cut into a cylindrical pattern mask/aperture pattern by water jet from a single piece. Each mask element is a wedge with angular width of 360.0/150 degrees, inner radius of 44.92 cm and outer radius of 55.08 cm. The top and bottom rows do not contain any apertures. The aperture pattern with the best imaging performance[4] out of 100 randomly generated patterns with the properties discussed above was selected, shown in Figure 10 (left).

[4] As defined by a chi square value between reconstructed images and true images used as an input to Monte Carlo

Along the axis of the cylindrical mask are two 1” diameter by 1” deep cylindrical Stilbene organic scintillator detector pixels coupled to 2” Hamamatsu model 6094 PMTs shown in Figure 10 (right). The centers of the detector pixels are positioned 2” above and below the centerline of the mask (detector labels 0 and 1 respectively). The current signals of the PMTs are digitized by a CAEN DT5720 250 MHz, 14-bit digitizer and read out via USB by a laptop PC along with the encoder position also by USB in two separate threads. The digitizer and computer clocks are synchronized at the beginning of each measurement which are then used to assign a mask angular orientation to every recorded event. Pulse shape discrimination (PSD) allows the gamma-ray and fast neutron counts as a function of rotation angle to be separated in offline analysis.

Figure 10 – Photograph of the CONFIDANTE prototype (left) and 1” diameter x 1” deep Stilbene detector and PMT from Inrad Optics (right).

4.3. Proof-of-concept Simulations

Using modeling tools developed in the Time-encoded Imaging project, we generated a detector response matrix; essentially a set of probability density functions (PDFs) for the detector pixel modulation as a function of rotation angle for each source bin within the field-of-view. We then input the source distributions that are shown in the center panels of Figure 12, Figure 13, Figure 14, and Figure 16 and generated detector pixel count distributions by using the forward projection through the detector response matrix as a PDF for randomly generating detected events as a function of rotation angle. The resulting distributions for one of the detector pixels are shown in the top left panels and the distribution of count values from all angle bins from both detector pixels are shown in the top right panels of the same figures.

---

simulations. The true image test patterns used were 20 cm diameter circular ring sources at 5 different vertical displacements (0,20), (0,10), (0, 0), (0, -10), and (0, -20).

A positive confirmation of two properly positioned identical objects is indicated by a count value distribution consistent with only statistical (Poisson) noise. To illustrate this, we do two things:

1. Plot the Poisson expectation (red line) as a visual indication of the expectation.
2. Calculate a test statistic to quantify how Poisson-like the distribution is. The Feynman Y value is defined as the ratio of the distribution's variance to its mean minus one ($Feynman\ Y = \left(\frac{variance}{mean} - 1\right)$). A Poisson distribution has a variance equal to its mean value and will therefore have a Feynman Y of zero.

Finally, we use the detector response matrix and the MLEM reconstruction method (9) to attempt to produce an image from the detector pixel count. These reconstructions, shown in the bottom panel of each figure, should not produce an image if the sources have effectively canceled each other out. Otherwise, they indicate that some information regarding the spatial distribution of source material is present in the detector pixel modulation.

For these examples, we used an unclassified object defined for the Workshop on Techniques for Protection of Imaging Information as our TAI. Details of this Workshop can be found in the conference proceedings of the INMM 57th annual meeting (10). A more detailed description of the challenge problem and TAI can be found here (11). Figure 11 provides the dimensions of the object. Pretendium is a fictional material with the mass density of tungsten, radiation interaction cross-sections of lead, neutron emission rate of 1e5 n/s/kg (Cf-252 emission spectrum), and gamma emission rate of 1e7 gamma-rays/s/kg (Eu-152 emission spectrum).

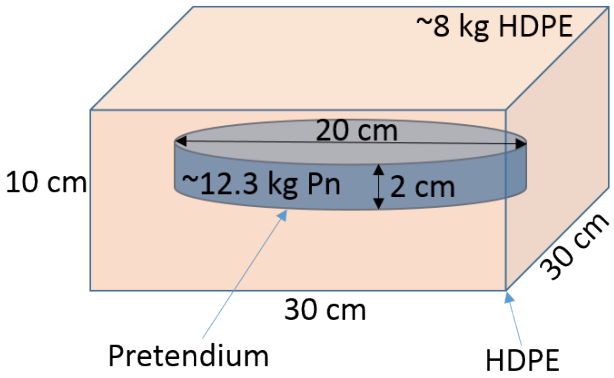


Figure 11 – (Not to scale) The type 1 TAI defined for the Workshop on Techniques for Protection of Imaging Information contains a cylinder of neutron and gamma-ray emitting material centered within a block of HDPE.

The challenge problem presented in the Workshop included the confirmation that a declared TAI, labeled X, is identical to reference object T that has previously been presented to the inspecting parties; reference measurements were allowed if information barriers (IBs) were enforced to protect declared sensitive information (the diameter of the Pretendium disk in this case). Further, a false TAI, labeled F, should not pass a confirmation measurement. A representative object F, used in this study, has the same mass of Pretendium with the same thickness (2 cm), but with a square rather than circular cross section.

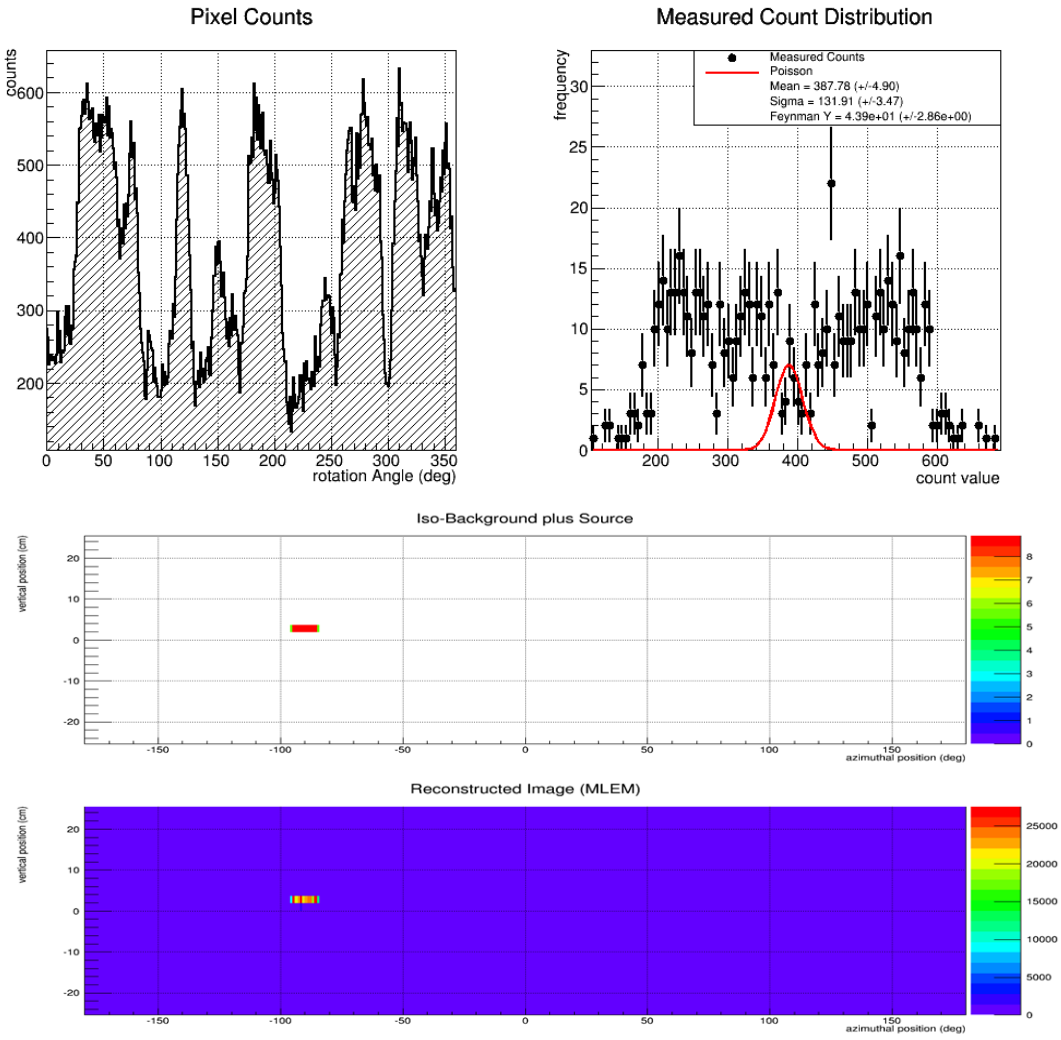


Figure 12 – Results from a simulation of a single TAI (T) centered at (-90, 3). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top, left panel. The red line is the expectation if the distribution were consistent with purely statistical (Poisson) noise. (Center) The true source distribution used to generate the pixel count values in the top, left panel. The y-axis is the vertical position in centimeters and the x-axis is the azimuthal angle in degrees. (Bottom) An MLEM reconstruction of the source distribution using the pixel count distribution in the top, left panel. The axes are identical to the center panel.

4.3.1. Single object (TAI T)

In Figure 12 we input a single object distribution centered at (-90,3) and viewed edge on. It can be seen that when only a single TAI is present, the pixel counts demonstrate strong modulation, the count values are far from being consistent with statistical noise with a Feynman Y value of 43.9 ± 2.86, and the counts as a function of rotation angle can be used to reconstruct an image (bottom panel). This demonstrates that a 2D-TEI with a mask pattern designed with these specific properties is capable of functioning as a two-dimensional imager and is thus sensitive to the spatial distribution of nuclear material within the TAI.

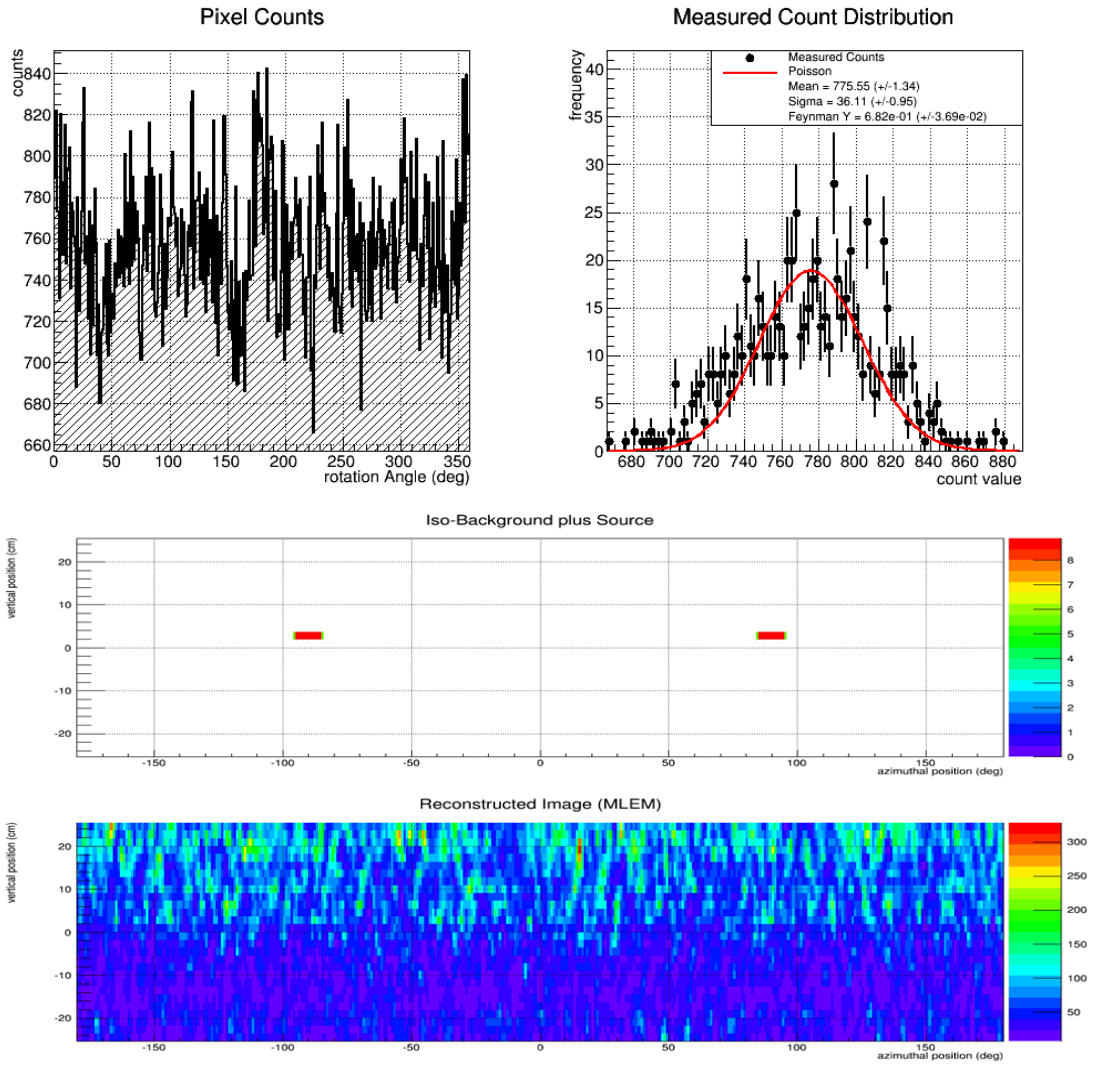


Figure 13 – Results from a simulation of a two identical objects (true TAI X vs. T) centered at (-90, 3) and (90, 3). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top, left panel. The red line is the expectation if the distribution were consistent with purely statistical (Poisson) noise. (Center) The true source distribution used to generate the pixel count values in the top, left panel. The y-axis is the vertical position in centimeters and the x-axis is the azimuthal angle in degrees. (Bottom) An MLEM reconstruction of the source distribution using the pixel count distribution in the top, left panel. The axes are identical to the center panel.

4.3.2. Two Identical objects (X vs. T)

In Figure 13 we input two identical objects (TAI X vs. T) positioned 180 degrees apart (on opposite sides of the system). It can be seen visually that the count value distribution (top, right) is reasonably consistent with the Poisson expectation and the calculated Feynman Y value is 0.682 ± 0.0369. We then simulated 1,000 independent trials of these two identical objects. The distribution of Feynman Y values is shown in Figure 15 (black curve). A threshold on this value,

can be used to indicate confirmation. Furthermore, even if one considers the entire count distribution as a function of rotation angle, Figure 13 (top, left), it is not possible to reconstruct the source distribution as can be seen in the bottom panel. The pattern from one of the sources (seen in Figure 12 top, left) is the complement of the other, so their addition effectively negates the other.

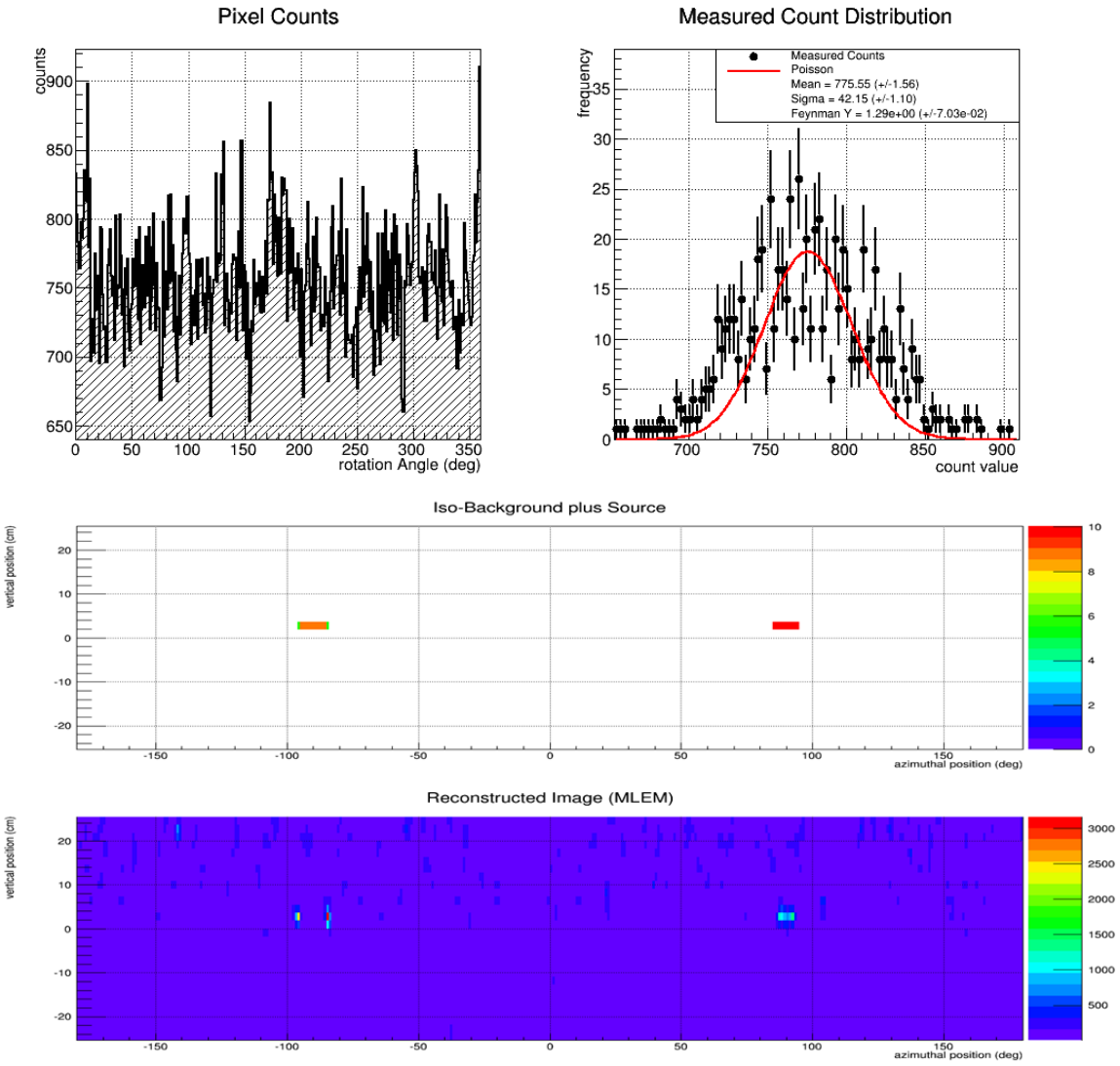


Figure 14 – Results from a simulation of a two dissimilar objects (false TAI F vs. T) centered at (-90, 3) and (90, 3). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top, left panel. The red line is the expectation if the distribution were consistent with purely statistical (Poisson) noise. (Center) The true source distribution used to generate the pixel count values in the top, left panel. The y-axis is the vertical position in centimeters and the x-axis is the azimuthal angle in degrees. (Bottom) An MLEM reconstruction of the source distribution using the pixel count distribution in the top, left panel. The axes are identical to the center panel.

4.3.3. Two different objects (F vs. T)

In Figure 14 we input two objects; however one is inconsistent with our definition of TAI, labeled F. Again, it can be seen that the count value distribution (top, right) is not consistent with being Poisson (Feynman Y = 1.29 ± 0.07). Additionally, if the count distribution as a function of rotation angle (top, left) is used to reconstruct an image (bottom), the difference set of both objects is apparent.

Again, 1,000 independent trials were simulated. The distribution of Feynman Ys is shown in Figure 15 (blue curve). It can be seen that object F is sufficiently different in its spatial distribution of nuclear material that it can readily be distinguished from a true TAI, T, by requiring that the Feynman Y value from a confirmation measurement be larger than a value ~0.9; while maintaining a high efficiency to confirm a true TAI, X.

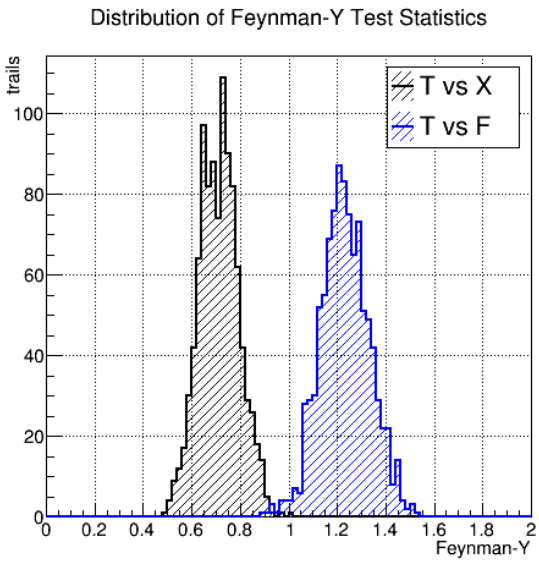


Figure 15 – Distribution of the Feynman-Y test statistic from 1,000 simulated trials (5e5 total counts each) of object X vs. reference object T (black) and object F vs. reference object T (blue).

As a measurement certification issue, it is likely that a host party will want to mitigate against a negative result leaking sensitive information. They may therefore seek to sequester this count distribution to prevent the monitoring party from creating an image in the event of a failed confirmation. With this in mind, a data acquisition system could be developed that sequentially updates an estimate of the Feynman Y and does not save the full count distribution. This could be achieved on a relatively simple ASIC, eliminating the need for any digital computer and making authentication more tractable.

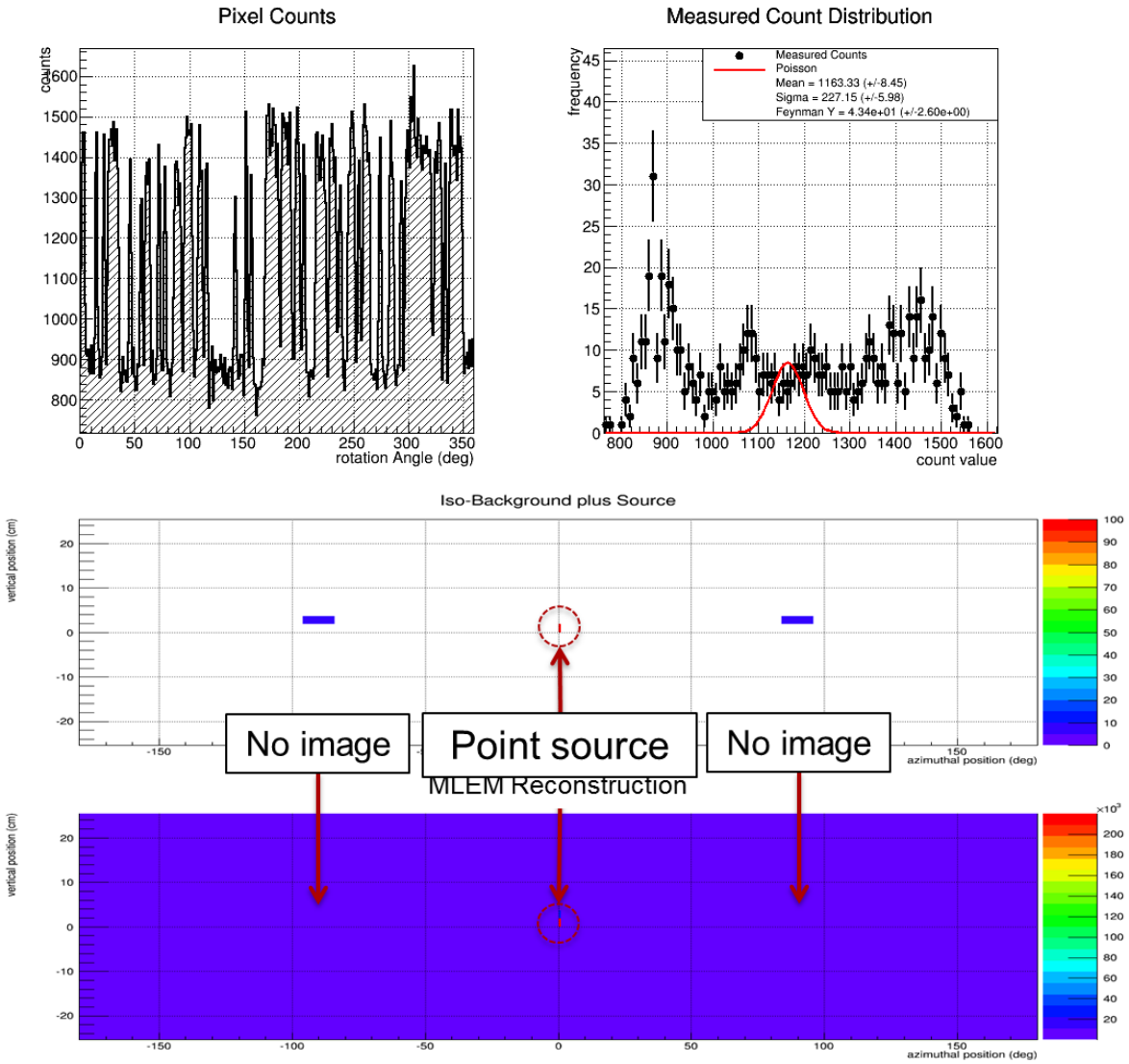


Figure 16 – Results from a simulation of a two identical objects (TAI X vs. T) centered at (-90, 3) and (90, 3) and a single point source at (0, 0). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top, left panel. The red line is the expectation if the distribution were consistent with purely statistical (Poisson) noise. (Center) The true source distribution used to generate the pixel count values in the top, left panel. The y-axis is the vertical position in centimeters and the x-axis is the azimuthal angle in degrees. (Bottom) An MLEM reconstruction of the source distribution using the pixel count distribution in the top, left panel. The axes are identical to the center panel.

4.3.4. Two identical objects plus a point source

Lastly, in Figure 16 we input two identical objects (TAI X vs. T) that should produce a true positive confirmation results and also add an additional point source. This demonstrates that, even as the two identical objects positively cancel each other out, the system is still functional as an imager. As seen in the lower panel, the point source image can still be reconstructed from the detector pixel modulation, but there is no remaining modulation from either object. This enables

measurement authentication procedures to be enacted; for example, the monitoring party may be allowed to position their own source and confirm that the image is consistent with its known location during the confirmation measurement. Such a measure would lend strong confidence that the equipment is functional and a measurement is taking place.

4.4. Prototype Measurement Results

The prototype imaging system described in 4.2.2 was used in a series of measurements to prove the feasibility of the CONFIDANTE concept. Measurements of single and multiple ^{252}Cf fission sources were made in the laboratory at Sandia National Laboratories, CA as well as a set of plutonium dioxide hemispherical shells, or Hemis, at Lawrence Livermore National Laboratory (LLNL). The ^{252}Cf fission sources are matched in activity to within 5% with an estimated neutron output of ~7.5e4 n/s each at the time of the measurements. The Plutonium dioxide Hemis, shown in Figure 17, are each plutonium dioxide hemispherical shells. These were used in configurations where the hemispheres were imaged separately on opposite sides of CONFIDANTE as well as fit together to form a single complete spherical shell.

A summary of the source configurations that were measured, the total dwell time of the measurements, and the estimated Feynman Y values obtained from the count distributions of both detector pixels over the each measurement are provided in Table 1. It can be seen that source configurations in which a single object is positioned on one side of the system are measured produce much larger Feynman Y values than those configurations in which two objects are positioned on opposite sides of the system; the smallest values originating from identical objects. This is consistent with the Monte Carlo predictions described in the previous section. Details of each measurement are provided in the following sub sections.

Figure 17 – Photograph of the two plutonium dioxide Hemispherical shells that were measured at LLNL.

Table 1 – Summary of measurements made, total dwell time, and Feynman Y values.

Object measured	Total dwell time (hours)	Feynman Y
Single ^{252}Cf source	20	5.31 ± 0.325
Single ^{252}Cf source + same run with 180 degree shift	10 (equivalent)	0.0731 ± 0.00412
Two ^{252}Cf sources positioned 180.0 degrees apart	22	0.233 ± 0.0128
Two ^{252}Cf sources positioned 177.5 degrees apart	22	0.555 ± 0.0307
Two ^{252}Cf sources positioned -55.5 and -44.5 degrees	20	5.98 ± 0.359
Two ^{252}Cf sources positioned 126.0 and 137.5 degrees	22	6.50 ± 0.392
Two ^{252}Cf sources sum of -55.5/-44.5 and 126.0/137.5 runs	20 (each)	0.0879 ± 0.00478
One PuO_2 spherical shell at 130 degrees	16.7	0.295 ± 0.0193
One PuO_2 spherical shell at -50 degrees	16.7	0.373 ± 0.0248
Sum of PuO_2 spherical shell at 130 degrees + same run with 180 degree shift	8.4 (equivalent)	0.0558 ± 0.00350
Sum of PuO_2 Sphere at 130 degrees and -50 degrees	16.7 (each)	0.0286 ± 0.00174
Two Hemis positioned 180 degrees apart	68.4	0.0176 ± 0.00103
One Hemi + rotated Hemi positioned 180 degrees apart	48.4	0.229 ± 0.0137

4.4.1. Single Point Source Measurements

In order to first demonstrate that the CONFIDANTE prototype functions as a fast neutron imaging system, a single ^{252}Cf fission "point" source was measured. The source was positioned vertically just below the midline of the mask and at -50 degrees azimuthally. Figure 18 (top row) shows the measured fast neutron count rate distributions for detector labels 0 (left) and 1 (center) as a function of the rotation angle of the mask.

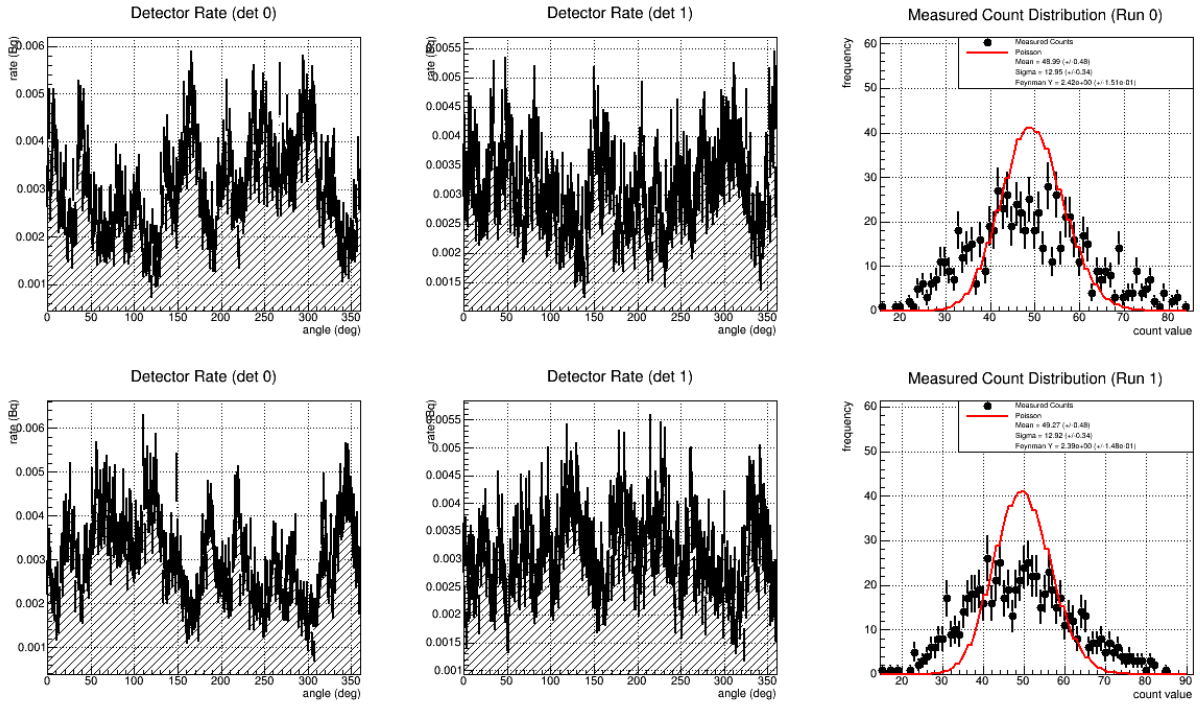


Figure 18 – (Left and center columns) Detector pixel fast neutron count rates as a function of rotation angle for detector 1 (left) and detector 2 (center) for a single ^{252}Cf source at -50.0 degrees (top row) and the same run shifted in phase by 180 degrees (bottom row). The right column is a histogram of the detector pixel counts summed over all angles. The red curves represent the Poisson noise expected for random counts.

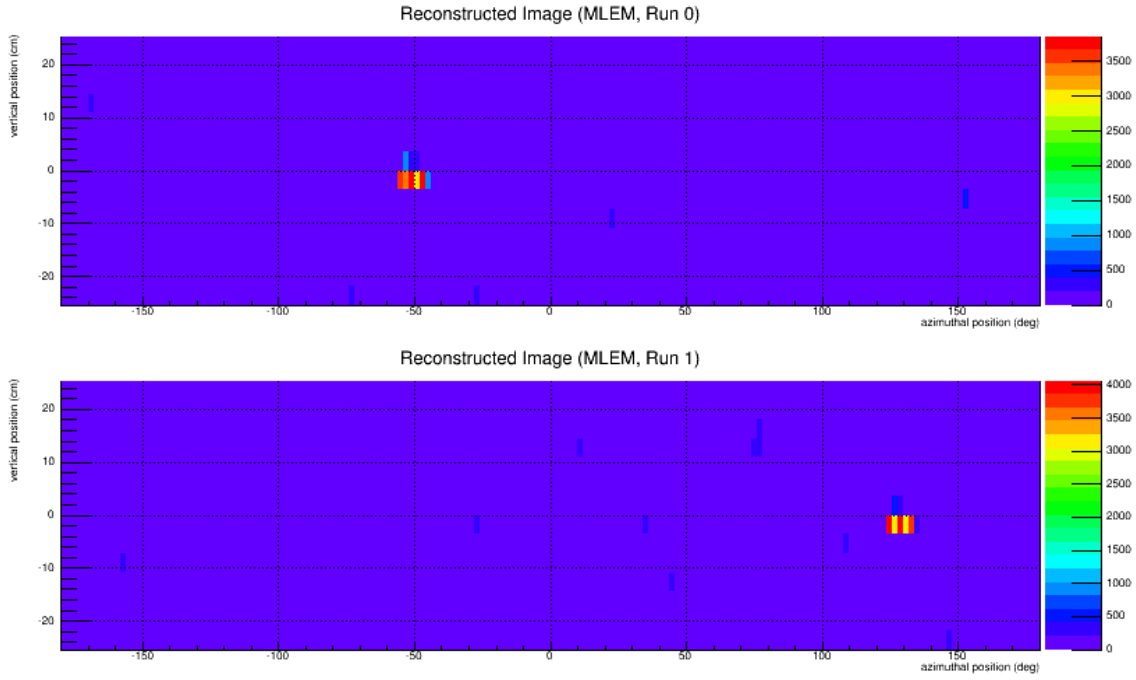


Figure 19 – MLEM reconstruction of a single ^{252}Cf point source at -50.0 (top) and MLEM reconstruction of events thrown from the same measurement with a 180-degree phase shift (bottom).

The distribution of count values in both detectors is shown in Figure 18 (right). It can be seen by comparing to the expected Poisson noise distribution, that this measurement is far from random with a Feynman Y value of 5.31 ± 0.325. In fact, as can be seen in Figure 19 (top), these distributions encode all of the information necessary to reconstruct an image of the point source at the expected location.

In order to demonstrate the principle that an identical point source positioned on the opposite side of the system will effectively cancel out the contribution from the first point source, resulting in only random Poisson distributed counts, we synthesized a second data set by randomly splitting this data set into two pieces; one of which is shifted in mask rotation angle by 180 degrees. This phase-shifted data set is shown in Figure 18 (bottom row). As expected, this modulation pattern reconstructs to an image of the point source with a 180 degree shift as shown in Figure 19 (bottom).

It can also be seen that the modulation pattern in the phase-shifted data is nearly an exact inverse of the original data and the sum of the two, shown in Figure 20 (left and center), produces a count rate distribution that is highly consistent with being purely Poisson in nature; as indicated by a Feynman Y value of 0.0731 ± 0.00412.

We next attempt to reconstruct an image from the count values as a function of rotation angle of the sum of the point source and the phase-shifted point source. In order to demonstrate that the resulting image, shown in Figure 21 (top), is consistent with noise, we generated 10,000 randomized trials from the data set using a bootstrapping technique (random selection from the original count distributions with replacement) and plot the MLEM reconstructed image divided by the standard deviation of each pixel, displayed in Figure 21 (bottom). It can be seen that there is not a significant excess with respect to statistical noise at the expected locations of the sources when compared to background pixels.

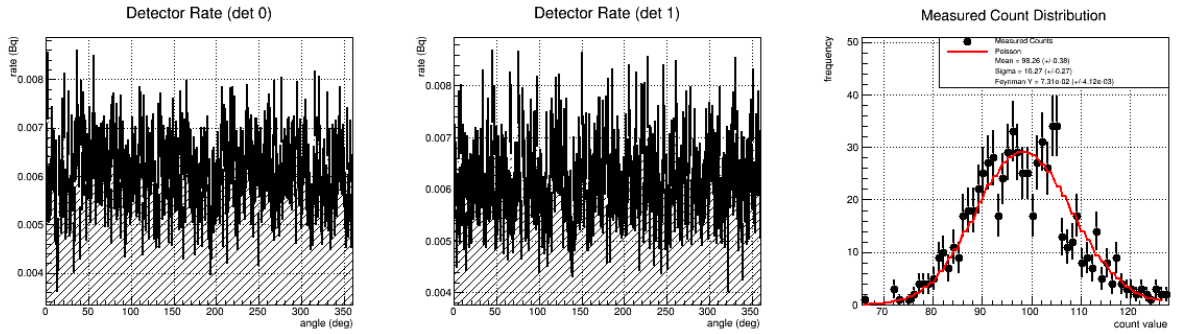


Figure 20 – Detector pixel fast neutron count rates as a function of rotation angle for detector 1 (left) and detector 2 (center) for the sum of a ^{252}Cf source at -50.0 degrees and the events drawn from the same data set shifted in phase by 180.0 degrees. (Right) A histogram of the detector pixel counts summed over all angles. The red curve represents the Poisson noise expected for random counts.

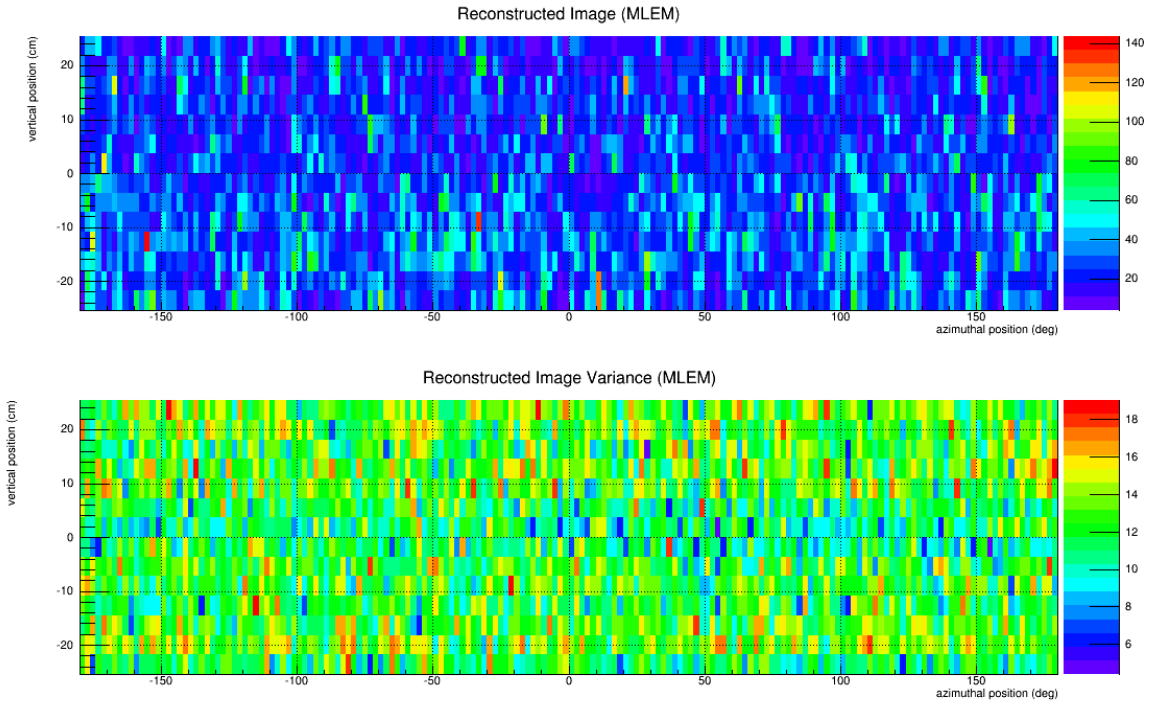


Figure 21 – MLEM reconstruction of the sum of a single ^{252}Cf point source at -50.0 and events thrown from the same measurement with a 180.0 degree phase shift (top) and the same image divided by the standard deviation of each pixel estimated over 10,000 bootstrapped trials (bottom).

4.4.2. Two Point Source Measurements

In this section, we present the results of measurements using two matched ^{252}Cf fission sources. In the first set of measurements, we demonstrate the principle that two identical sources positioned on opposite sides of the system will effectively cancel each other out. In order to align the two sources, the CONFIDANTE prototype was outfitted with two adjustable arms with source holders on each side of the system and a laser pointer affixed to the mask (shown in Figure 22). The mask was rotated to the desired angular position of the first source and then rotated by 180 degrees to point to the position of the second source. The arms were then adjusted such that the laser spot aligned to the same position on each source. The distance to each source was determined using a tape measure. In all measurements, a distance of 16” from the outer surface of the mask was used.

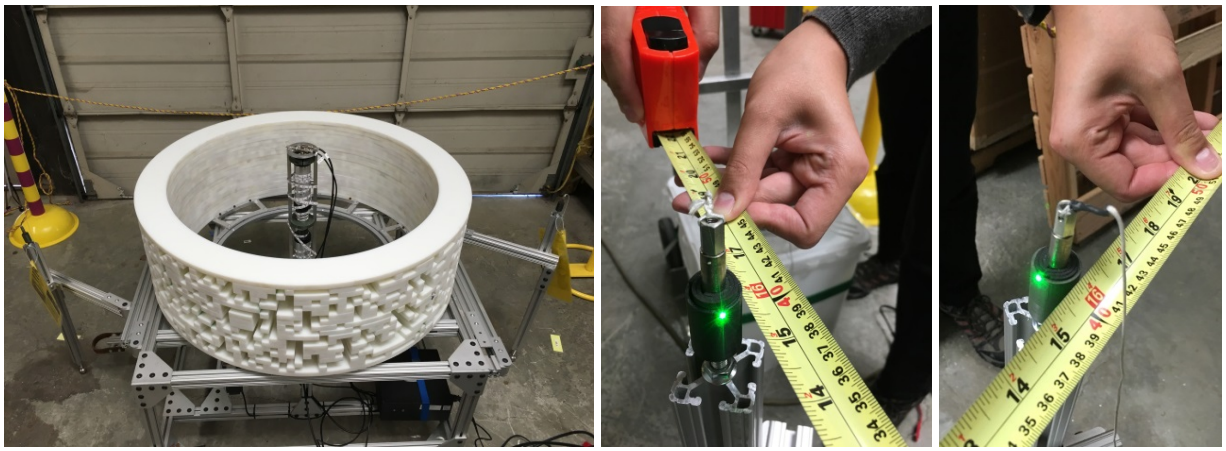


Figure 22 – Photograph of CONFIDANTE measuring two ^{252}Cf point sources aligned 180 degrees apart on opposite sides (left). The sources fit into holders built into adjustable arms attached to the imager's frame (center and right). To align the sources, a laser affixed to the mask and a measuring tape was used.

Following this alignment procedure, a measurement was taken with the point two sources. The detector pixel fast neutron count rates and count distribution are shown in Figure 23. It can be seen that these distributions are reasonably consistent with a random Poisson count distribution giving a Feynman Y value of 0.233 ± 0.0128, however this is a larger value than that obtained in the previous section by synthesizing a data set.

This is most probably caused by errors in the calibration of the measured encoder position to true rotation angle. It was later found that the width of the switch that resets the encoder position to zero on each rotation is approximately 1.5 degrees wide and therefore the 360 degrees shown in each of the figures is actually approximately 358.5 degrees. This causes an approximate 0.75 degree misalignment of the second source with respect to the first when using the aforementioned alignment procedure. Nevertheless, the reconstructed image shown in Figure 24 is reasonably random with no pixels deviating significantly with respect to expected background fluctuations.

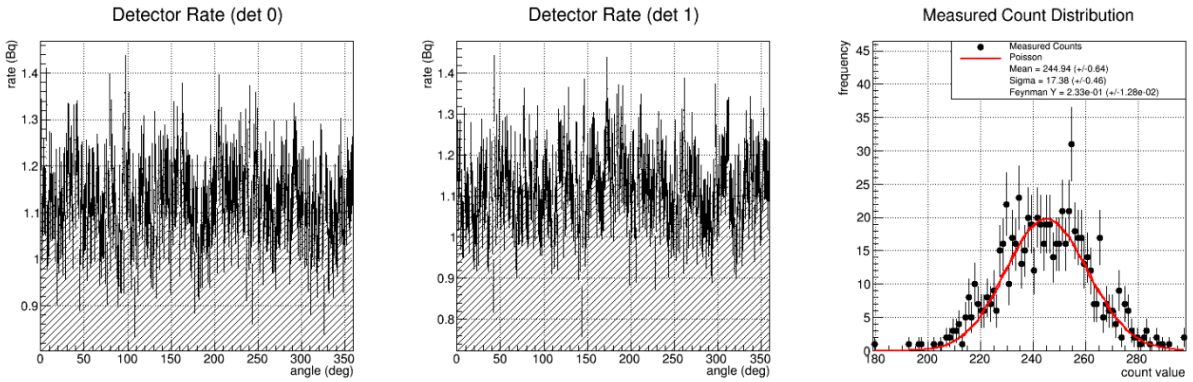


Figure 23 – Detector pixel fast neutron count rates as a function of rotation angle for detector 1 (left) and detector 2 (center) for the sum of a ^{252}Cf source at -50.0 degrees and a second ^{252}Cf source at 130.0 degrees. (Right) A histogram of the detector pixel counts summed over all angles. The red curve represents the Poisson noise expected for random counts.

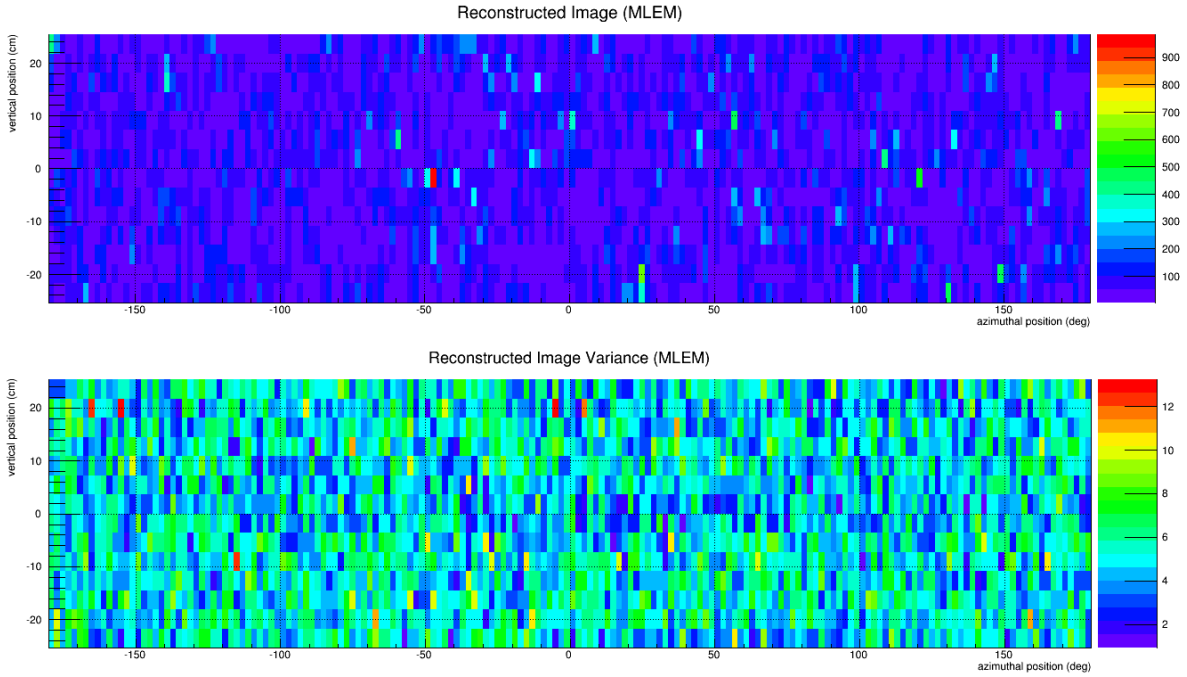


Figure 24 – MLEM reconstruction of a ^{252}Cf point source at -50.0 degrees and a second at 130.0 degrees (top) and the same image divided by the standard deviation of each pixel estimated over 10,000 bootstrapped trials (bottom).

Figure 25 and Figure 26 show the detector pixel count distributions and MLEM reconstructed image (respectively) for two point sources misaligned from 180 degrees by approximately 2.5 degrees. At approximately the intrinsic resolution of the imaging system, these sources are easily discernable with a Feynman Y value of 0.555 ± 0.0307. Additionally, the reconstructed image reveals the location of both sources, highlighting the fact that information regarding the spatial distribution of the two objects being measured is at risk if they are not in fact identical.

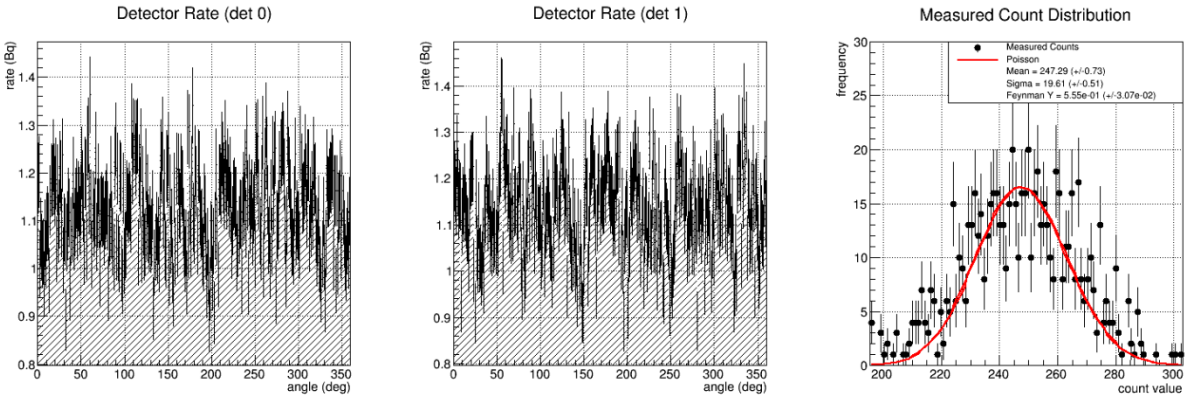


Figure 25 – Detector pixel fast neutron count rates as a function of rotation angle for detector 1 (left) and detector 2 (center) for the sum of a ^{252}Cf source at -52.5 degrees and a second ^{252}Cf source at ~125.0 degrees. (Right) A histogram of the detector pixel counts summed over all angles. The red curve represents the Poisson noise expected for random counts.

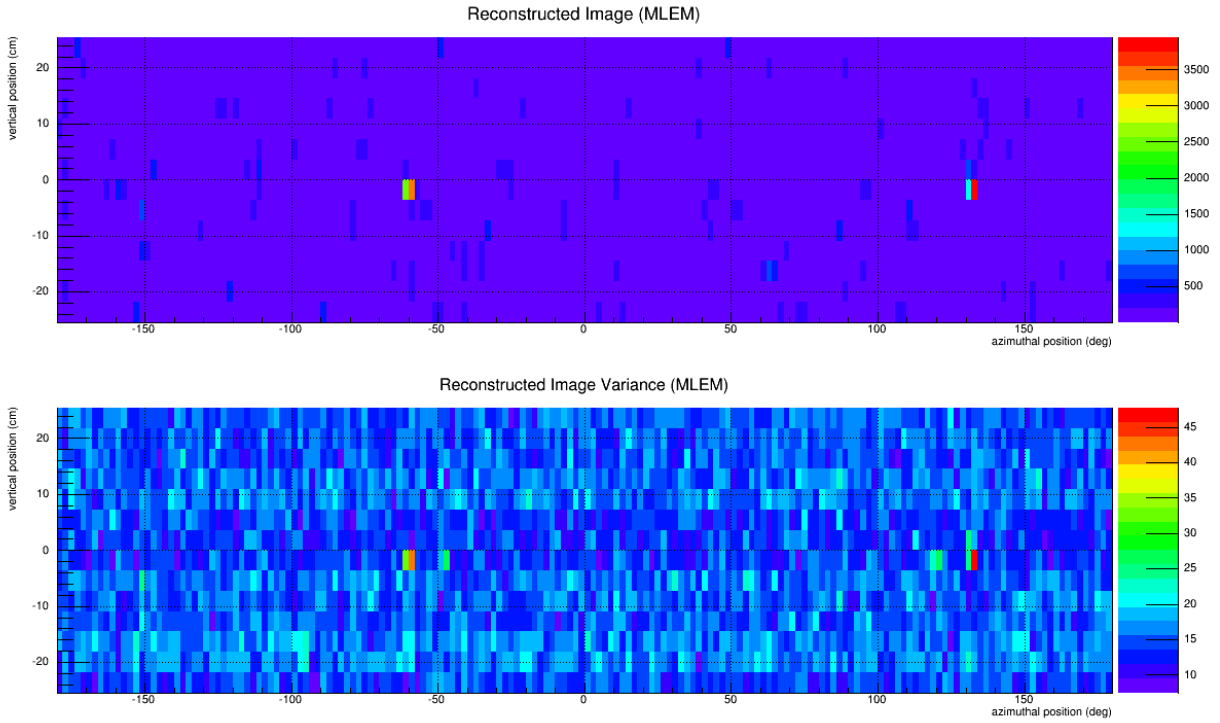


Figure 26 – MLEM reconstruction of a ^{252}Cf point source at -52.5 degrees and a second at ~125.0 degrees (top) and the same image divided by the standard deviation of each pixel estimated over 10,000 bootstrapped trials (bottom).

Next, a more extended source distribution was synthesized by positioning the two matched ^{252}Cf fission sources at -55 and -44.5 degrees and then again at 126.0 and 137.5 degrees (approximately 20 cm. separation at 16 inches from the outer diameter of the mask). Note that this is the width of the challenge object described in Section 4.3 and the reconstructed image of this configuration shown in Figure 28 is very similar to that of the simulation shown in Figure 12.

The detector pixel count rates and count distributions for each of the two positions shown in Figure 27 are again very far from being consistent with random Poisson counting statistics with Feynman Y values of 5.98 ± 0.359 and 6.50 ± 0.392 respectively. The reconstructed images shown in Figure 28 meet expectations in terms of angular position and width.

Finally, Figure 29 shows the detector pixel count distributions for the sum of these two data sets. As indicated by the very low Feynman Y value of 0.0879 ± 0.00478, these two objects cancel each other out quite well and the image reconstructed from their sum, seen in Figure 30, does not deviate significantly from random fluctuations across the entire field of view. This is a strong positive indication that these two source distributions are identical and properly aligned.

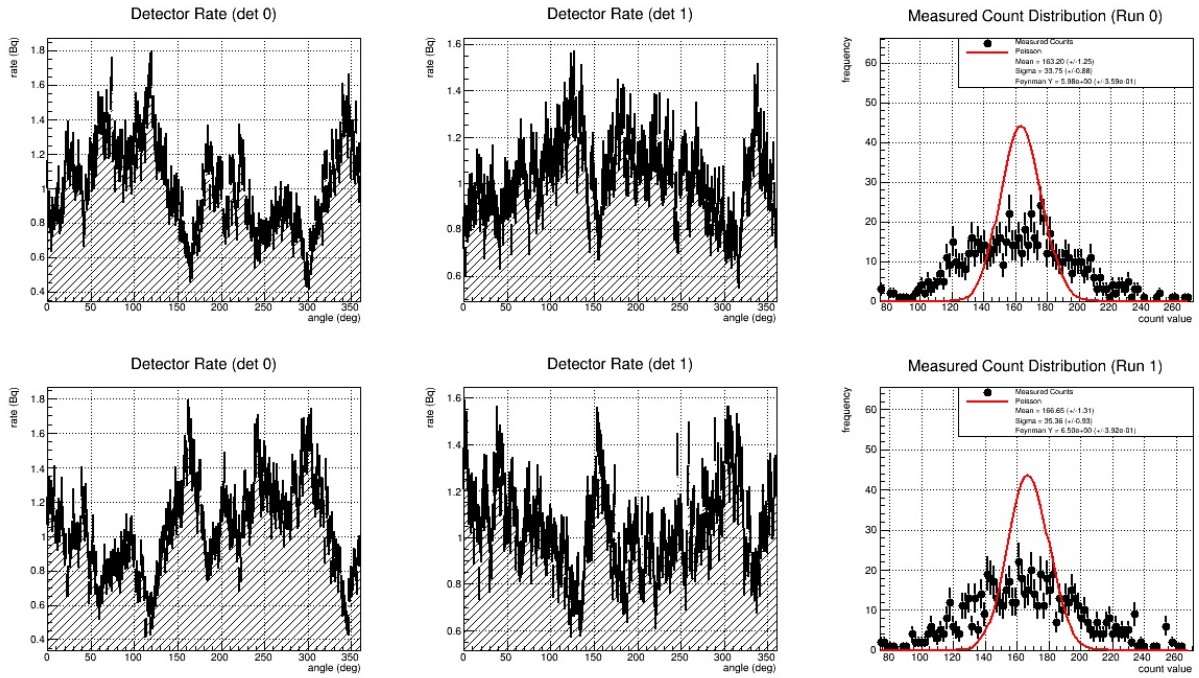


Figure 27 – (Left and center columns) Detector pixel fast neutron count rates as a function of rotation angle for detector 1 (left) and detector 2 (center) for two ^{252}Cf sources at -55.5 and -44.5 degrees (top row) and 126.0 and 137.5 degrees (bottom row). The right column is a histogram of the detector pixel counts summed over all angles. The red curves represent the Poisson noise expected for random counts.

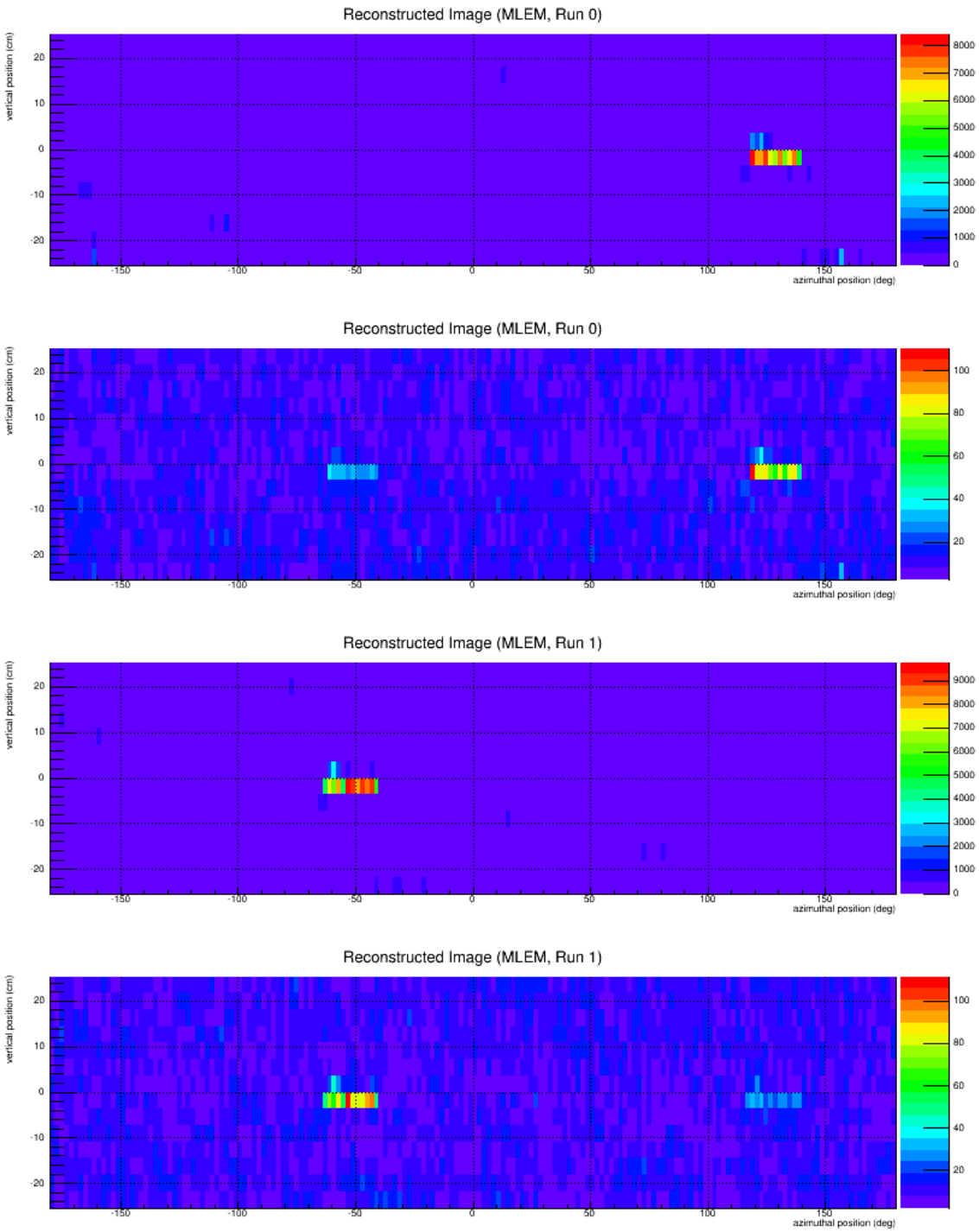


Figure 28 – MLEM reconstruction of two ^{252}Cf point sources at 126.0 and 137.5 (top) and the same image divided by the standard deviation of each pixel estimated over 10,000 bootstrapped trials (2nd from top). MLEM reconstruction of two ^{252}Cf point sources at -55.5 and -44.5 (3rd from top) and the same image divided by the standard deviation of each pixel estimated over 10,000 bootstrapped trials (bottom).

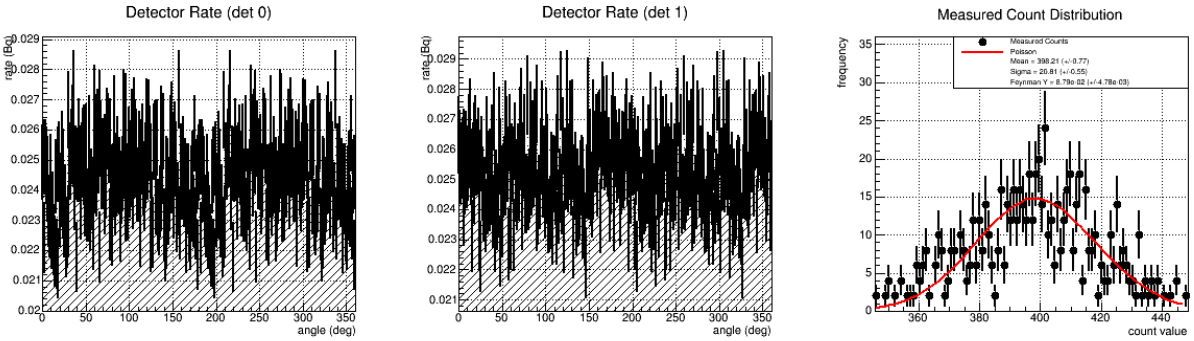


Figure 29 – Detector pixel fast neutron count rates as a function of rotation angle for detector 1 (left) and detector 2 (center) for the sum of two ^{252}Cf sources at -55.5 and -44.5 degrees and a second pair of ^{252}Cf source at 126.0 and 137.5 degrees. (Right) A histogram of the detector pixel counts summed over all angles. The red curve represents the Poisson noise expected for random counts.

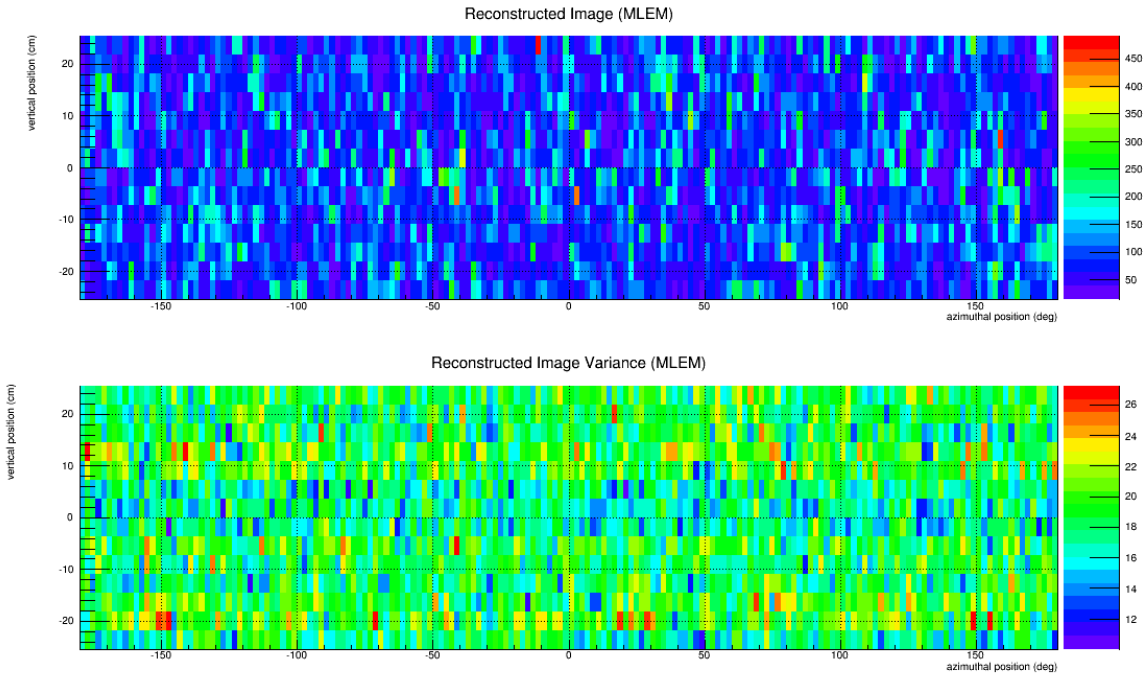


Figure 30 - MLEM reconstruction of two ^{252}Cf point sources at 126.0 and 137.5 degrees and a second set at -55.5 and -45.5 degrees (top) and the same image divided by the standard deviation of each pixel estimated over 10,000 bootstrapped trials (bottom).

4.4.3. Single Sphere Measurements

In this set of measurements, LLNL's plutonium dioxide Hemis were affixed together to form a single spherical shell with a total mass of approximately 380 grams. The single Pu sphere was positioned at approximately the centerline of the mask on a cork ring on a table as seen in Figure 31. The distance from the outer diameter of the mask to the center of the sphere was approximately 16 inches. Figure 32 shows a selected region of the separate fast neutron (left) and gamma-ray (right) image reconstructions of this spherical configuration. It should be noted that it can be discerned from the fast neutron image that this object is a hollow shell, but the gamma-ray image is more consistent with a solid sphere. This is caused by the self-attenuation of the gamma-rays within the Pu sphere such that only those emitted from the outer surface can escape to be detected by the system.

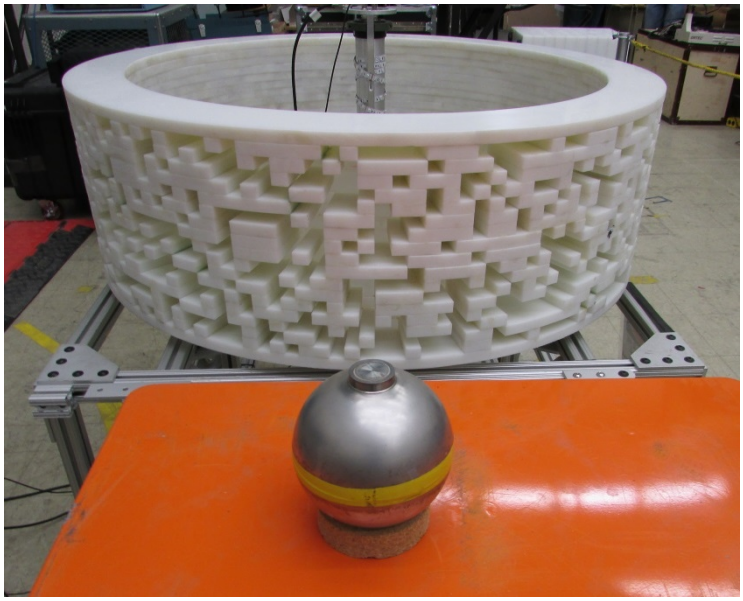


Figure 31 - Photograph of CONFIDANTE during a measurement of the two plutonium dioxide Hemispheres fit together to form a single sphere (foreground).

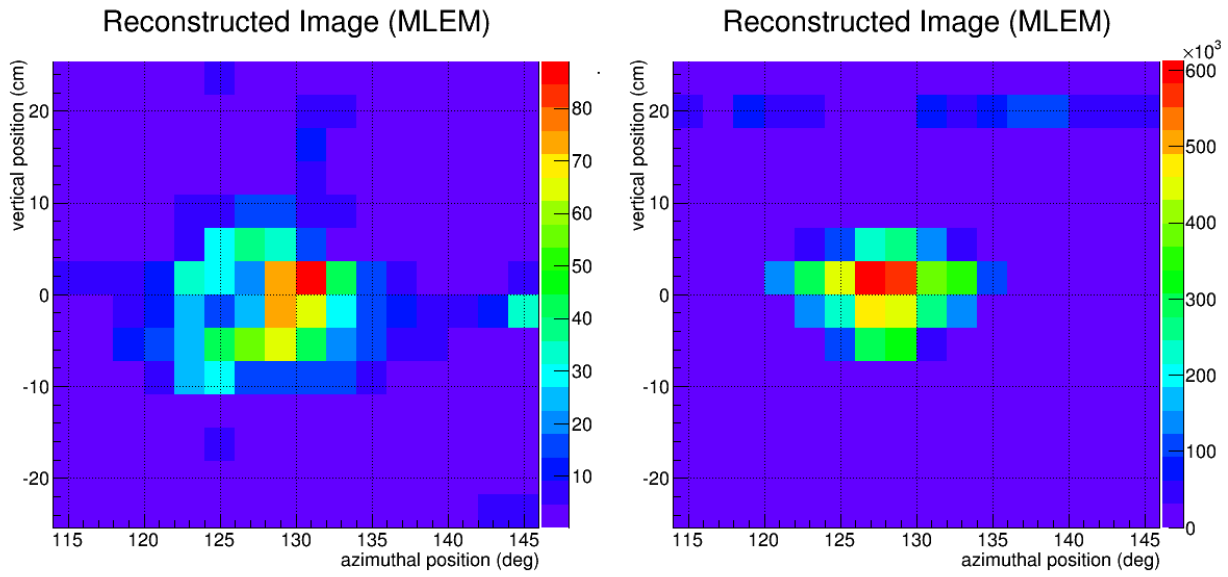


Figure 32 – Selected region of the fast neutron (left) and gamma-ray (right) MLEM reconstruction of a single PuO_2 spherical shell.

The Pu Dioxide spherical shell was measured at both 130 degrees and -50 degrees. First we demonstrate what can be achieved if one were able to perfectly position the two spherical shells on opposite sides of the system by randomly splitting the 130 degree measurement into two statistically independent data sets; one of which is given a 180 degree phase shift to the rotation angle. Figure 33 and Figure 34 show the detector pixel count rates of these two data sets and the MLEM reconstructed images respectively. As expected, the images reconstruct with a 180 degree shift in position.

When the two detector pixel count rate distributions are added together, synthesizing a single measurement of two identical sets of spherical shells with exact alignment, we get count distributions that are consistent with random counts; having a Feynman Y value of 0.0558 ± 0.00350 as shown in Figure 35. Figure 36 further demonstrates that there is no information regarding the spatial/angular distribution of Special Nuclear Material (SNM) remaining in the data. Fluctuations in the reconstructed image at the location of the spherical shells are consistent with those found in the background.

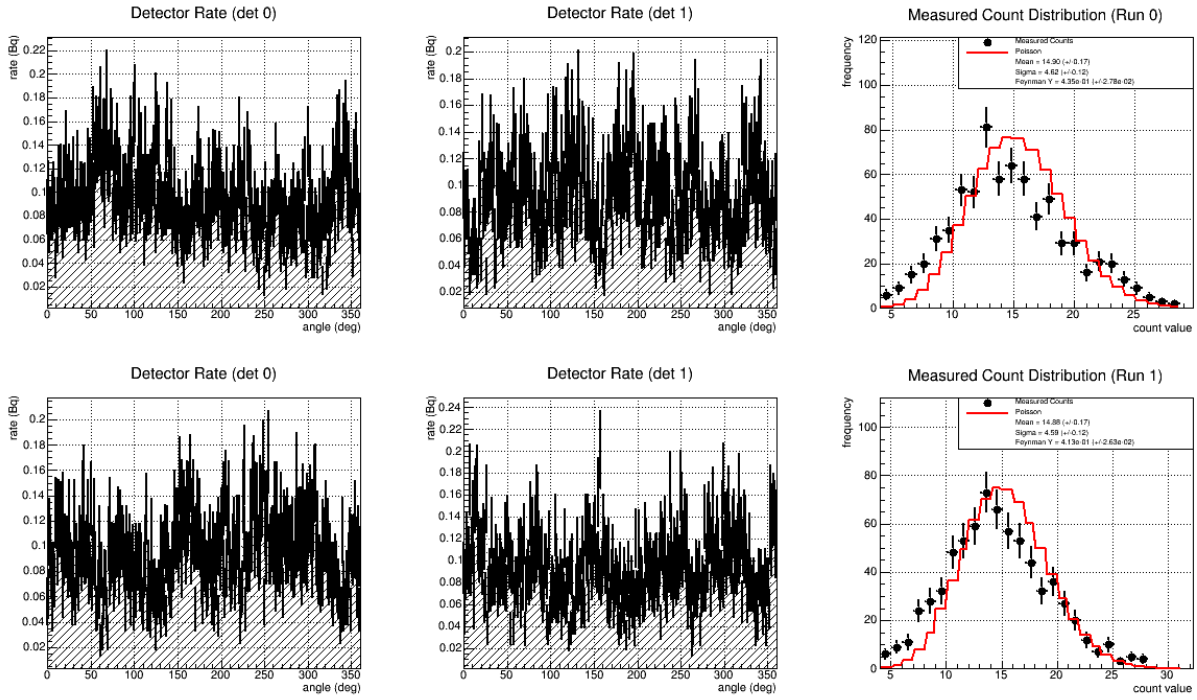


Figure 33 – (Left and center columns) Detector pixel fast neutron count rates as a function of rotation angle for detector 1 (left) and detector 2 (center) for one PuO_2 spherical shell at 130.0 degrees (top row) and a subset of events drawn from the same data set shifted in phase by 180.0 degrees (bottom row). The right column is a histogram of the detector pixel counts summed over all angles. The red curves represent the Poisson noise expected for random counts.

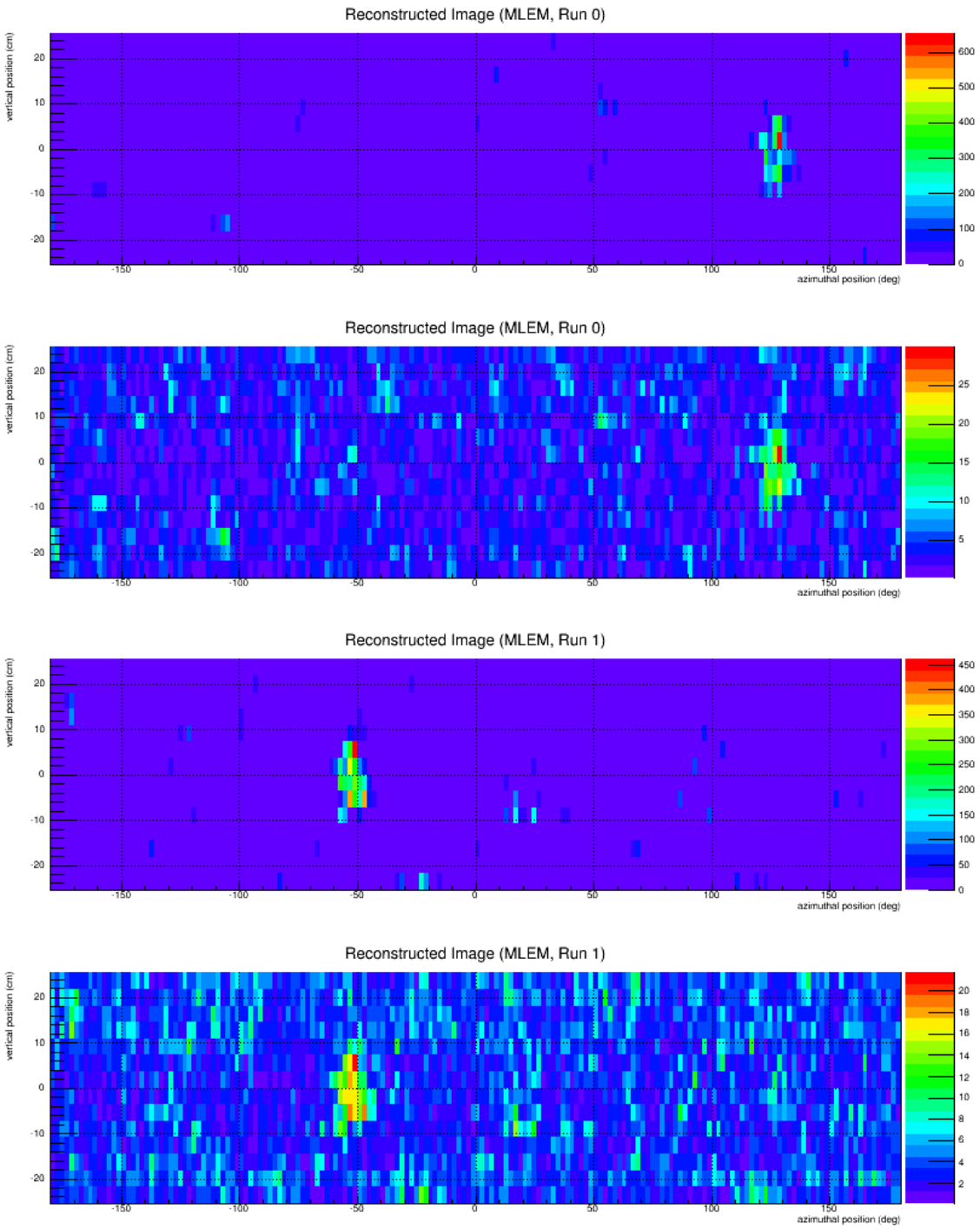


Figure 34 – MLEM reconstruction of one PuO_2 spherical shell at 130.0 (top) and the same image divided by the standard deviation of each pixel estimated over 10,000 bootstrapped trials (2nd from top). MLEM reconstruction of events thrown from the same measurement with a 180 degree phase shift (3rd from top) and the same image divided by the standard deviation of each pixel estimated over 10,000 bootstrapped trials (bottom).

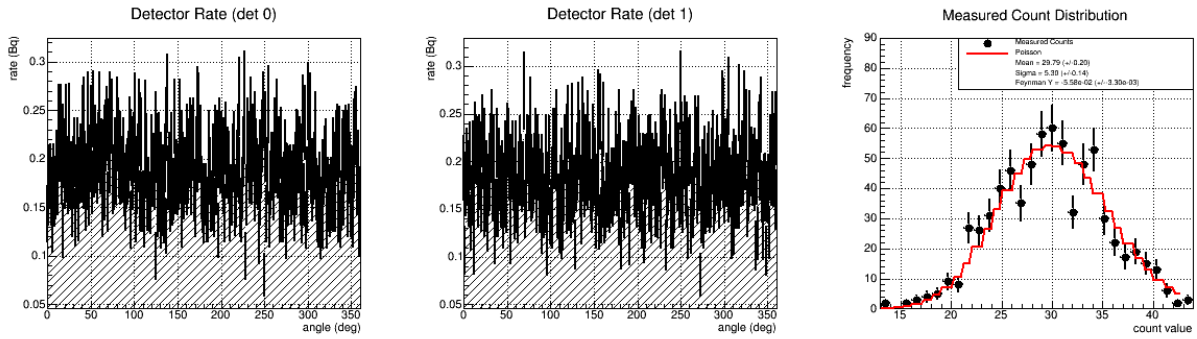


Figure 35 – Detector pixel fast neutron count rates as a function of rotation angle for detector 1 (left) and detector 2 (center) for the sum of the PuO_2 spherical shell at -50.0 degrees and the events drawn from the same data set shifted in phase by 180.0 degrees. (Right) A histogram of the detector pixel counts summed over all angles. The red curve represents the Poisson noise expected for random counts.

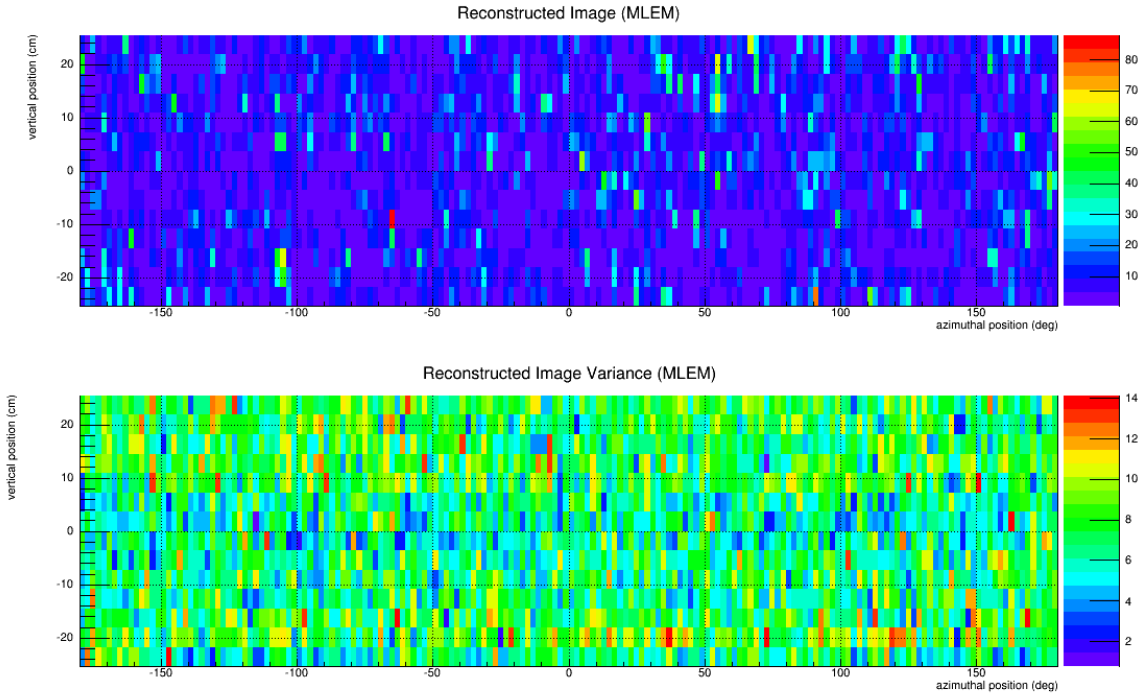


Figure 36 - MLEM reconstruction of the sum of one PuO_2 spherical shell at 130.0 and events thrown from the same measurement with a 180.0 degree phase shift (top) and the same image divided by the standard deviation of each pixel estimated over 10,000 bootstrapped trials (bottom).

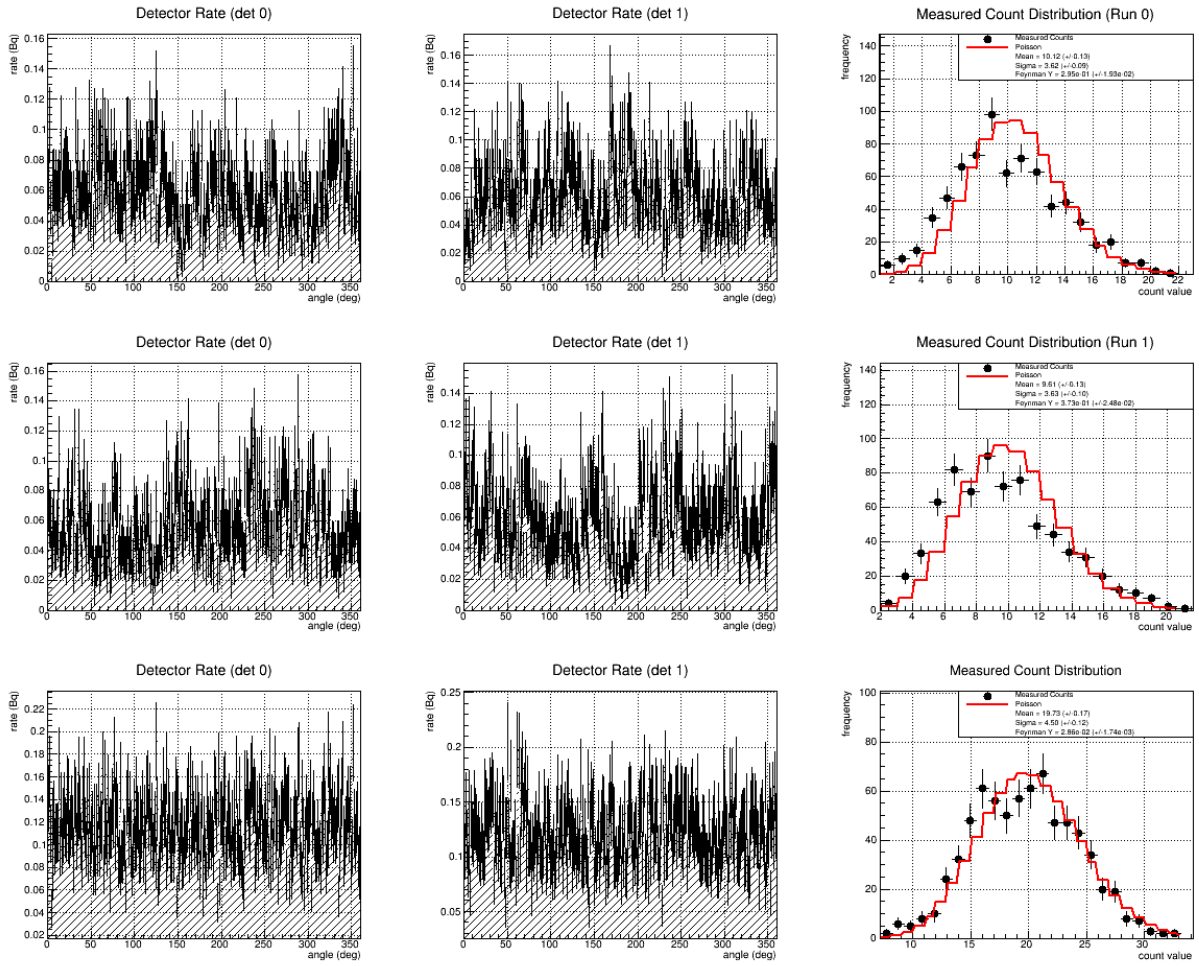


Figure 37 – (Left and center columns) Detector pixel fast neutron count rates as a function of rotation angle for detector 1 (left) and detector 2 (center) for one PuO_2 spherical shell at 130.0 degrees (top row), a second run at -50.0 degrees (center row) and the sum of the two (bottom row). The right column is a histogram of the detector pixel counts summed over all angles. The red curves represent the Poisson noise expected for random counts.

Next, rather than synthesizing a measurement by splitting a single data set into two pieces and phase-shifting half of the events by 180 degrees, we synthesize a measurement by adding two independent measurements in which the PuO_2 spherical shell was physically moved to the opposite side of the imaging system. The detector pixel count rates for the two separate measurements and the sum of the two measurements are shown in Figure 37. With a Feynman Y value of 0.0286 ± 0.00174, almost a factor of 2 lower than the phase-shifted synthesized data, this again is strongly consistent with random counting statistics.

The MLEM image reconstructions of the two independent measurements and the sum of the two are shown in Figure 38. It is clear that no remaining spatial/angular information is evident and an image cannot be formed.

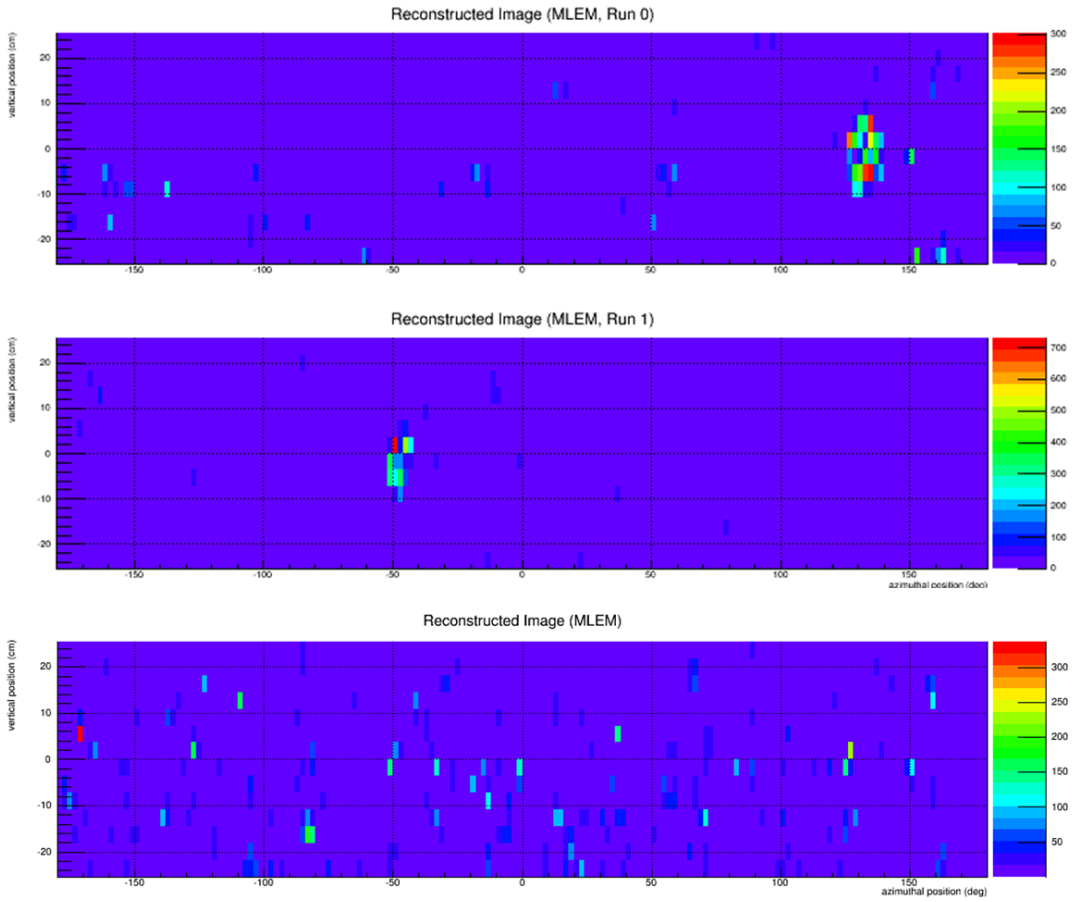


Figure 38 – The MLEM reconstruction of the plutonium dioxide Spherical Shell positioned at 130.0 degrees (top), -50.0 degrees (center), and the sum of the two data sets (bottom).

4.4.4. Two Hemisphere Measurements

In the last set of measurements presented here the two Hemis were positioned on opposite sides of the imaging system. As seen in Figure 39, the Hemis were taped to ½" thick high density polyethylene shells with the same diameter and oriented such that the PuO_2 shells faced the center of the system standing upright. This represents a true positive test case in which the two objects should be identical. Figure 40 shows the detector pixel count rates and MLEM reconstructed image. Again a low Feynman Y value of 0.0176 ± 0.00103 was obtained and both the count distribution and image indicate that the two Hemis have effectively canceled out each other's projected images; confirming that they are identical distributions.

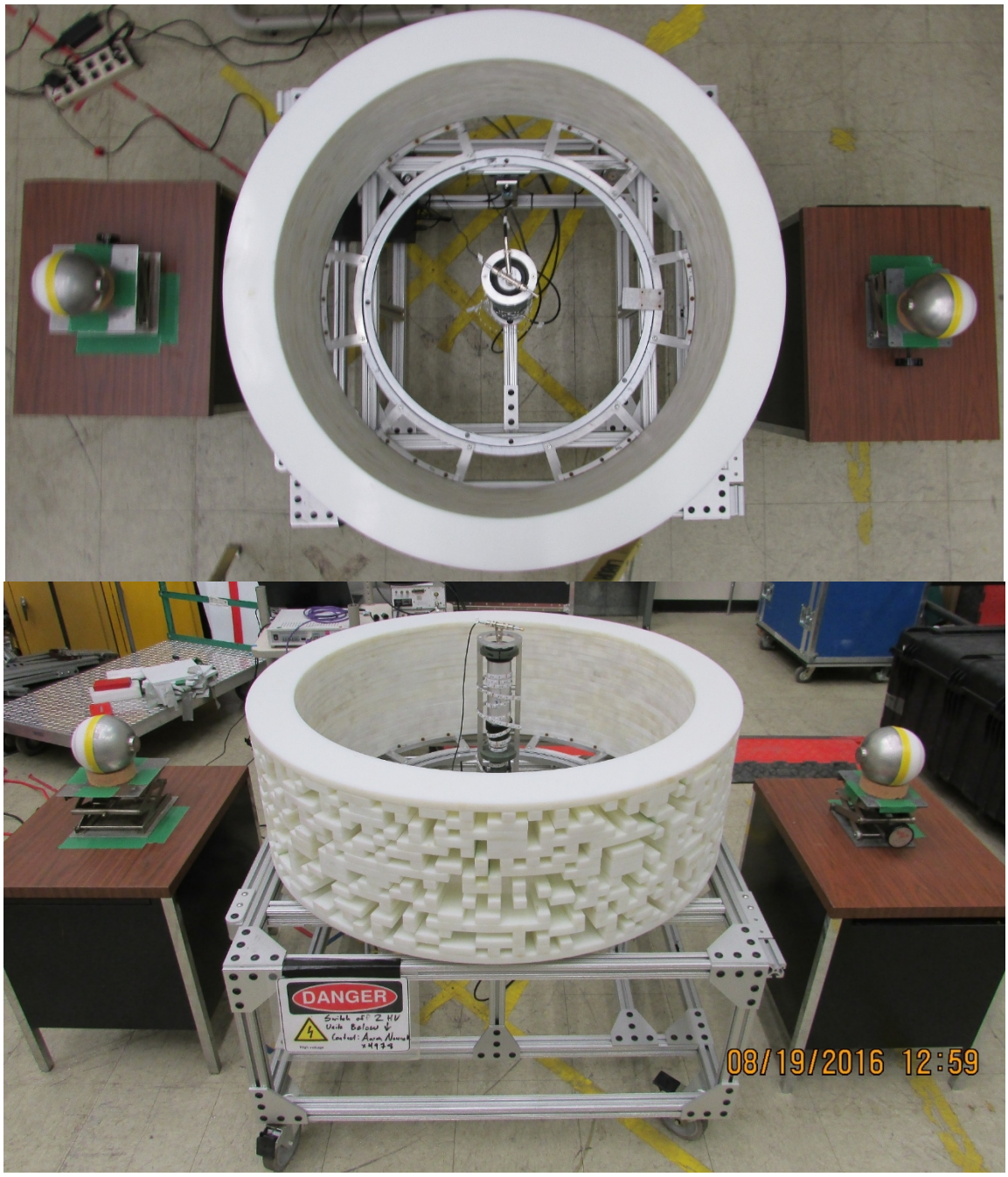


Figure 39 – Photographs of CONFIDANTE measuring two plutonium dioxide Hemis positioned 180 degrees apart on opposite sides of the system. Each Hemi is held upright by a half inch thick hemispherical shell of HDPE.

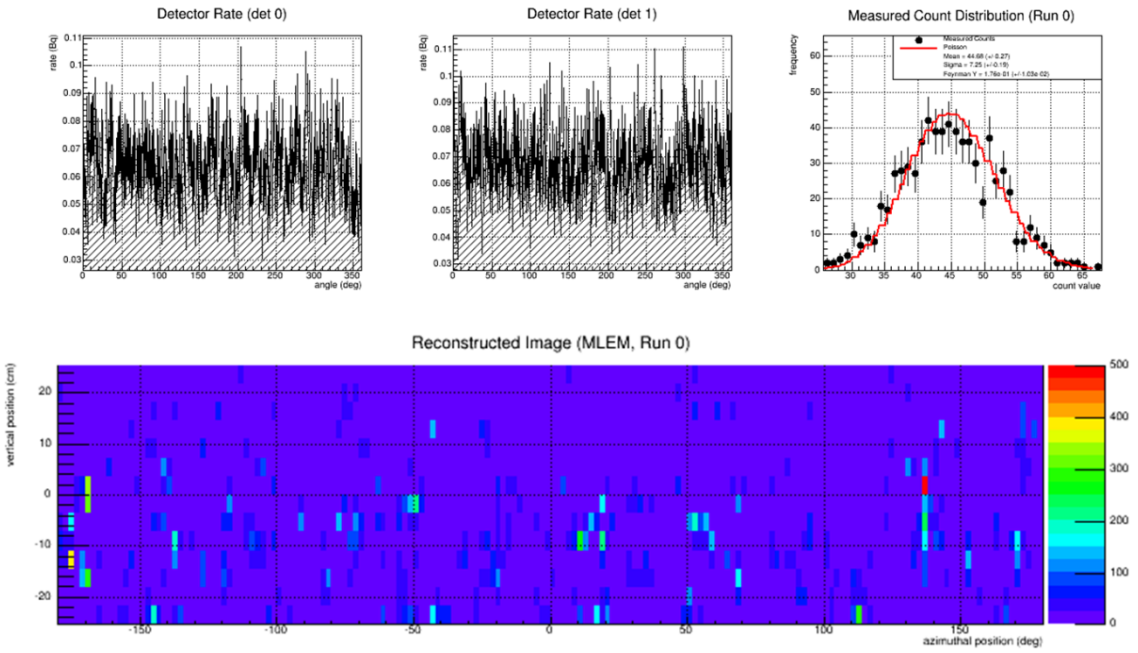


Figure 40 – (Top left and top center) Detector pixel neutron count rates as a function of rotation angle for two Hemis aligned on opposite sides of the system. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top left and top center panels. The red line is the expectation if the distribution were consistent with purely statistical (Poisson) noise. (Bottom) An MLEM reconstruction of the source distribution using the pixel count distribution in the top left and top center panels.

Finally, one of the Hemis was kept in the same orientation whilst the other was rotated by 90 degrees such that the PuO_2 shell faced downward with the HDPE hemi-shell on the top half. This represents a true negative test case in which the two objects are not identical. Figure 41 shows the detector pixel count rates and MLEM reconstructed image. The Feynman Y value of 0.229 ± 0.0137 is considerably higher than the true positive test case being almost as large as a measurement of a single PuO_2 sphere and the image clear reveals an excess below a vertical position of zero at ~-50 degrees and above zero at ~130 degrees. This is consistent with expectations given that the rotated object was at -50 degrees and presents an excess on the lower half of the shell. Because there is no neutron emitting material on the upper half of the rotated object, the upright object at 130 degrees presents an excess on the upper half.

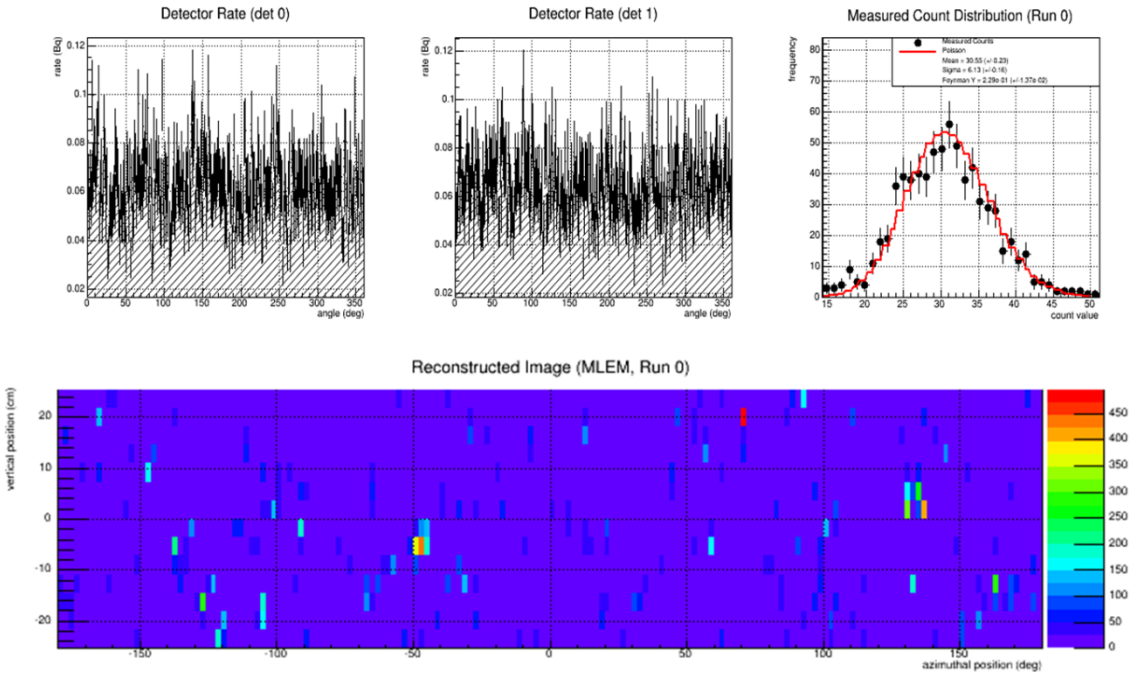


Figure 41 - (Top left and top center) Detector pixel neutron count rates as a function of rotation angle for two Hemis on opposite sides of the system; one of the Hemis has been rotated by 90 degrees such that it is lying on its rounded edge like a bowl. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top, left and center panels. The red line is the expectation if the distribution were consistent with purely statistical (Poisson) noise. (Bottom) An MLEM reconstruction of the source distribution using the pixel count distribution in the top left and top center panels.

In order to evaluate whether the Feynman Y value obtained in the measurement with one rotated Hemi is statistically different from that obtained with the two Hemis in the same orientation, we again utilize a bootstrapping technique to synthesize 10,000 trials from each of the measured detector pixel count distributions as a function of rotation angle by selecting a new random set of counts from each of them (with replacement). For each trial we calculate a new Feynman Y from the new detector pixel count distributions. However, because these distributions already contain random Poisson counting noise, the variance of the bootstrapped count rates contain twice the expected variance. We therefore divide the variance by a factor of two when calculating the Feynman Y value. The Feynman Y distributions for the 10,000 synthesized trials of each data set are shown in Figure 42. It can be seen that though they are reasonably separated, a threshold could not be chosen to simultaneously provide a low false positive and high true positive rate. The mean and full width half maximum (FWHM) of the aligned Hemi distribution is 0.0433 and 0.11 respectively and 0.138 and 0.12 for the rotated Hemi distribution. This provides a figure of merit (FOM) defined as the difference in means divided by the sum of FWHMs of 0.42. We expect that this FOM can be improved with higher counting statistics over longer measurements.

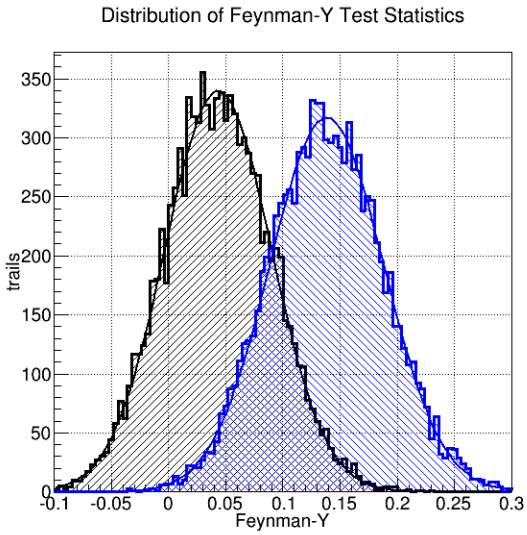


Figure 42 – The Feynman Y distribution from 10,000 trials synthesized from measurements of the Hemis aligned (black) and with one Hemi rotated by 90 degrees (blue). The solid curves are Gaussian fits through the distributions.

5. SOME OPEN QUESTIONS

Though the concepts presented in this work offer a promising option for warhead confirmation in support of potential future arms control treaty verification, there remain a few open questions and potential issues that warrant further investigation. The first, and perhaps most obvious, is how well aligned do the objects need to be in order to maintain the NULL-positive property. We have shown that a misalignment of two point sources by the intrinsic resolution of the system, approximately 2.5 degrees, is easily discernable. However, given enough statistics in the count distribution, it may be possible to detect even sub-resolution misalignment. Some degree of misalignment is inevitable, so the question should be answered statistically in terms of how long one must dwell (or how many events are required) to detect a deviation from a constant Poisson rate given an alignment imprecision, and what can be learned from that deviation.

The second open question is much like the first: what tolerance can be expected in the construction of the object containers or objects themselves? If that variation affects the modulation of fast neutrons in a significant way, then the NULL-positive condition may not be guaranteed.

Lastly, the property of object image/anti-image complement superposition as outlined in the Section 4.2.1 and illustrated in Figure 9 is only strictly true for a point detector at the center of the rotating cylindrical mask. As illustrated in Figure 43, the expected rate may briefly fluctuate during transitions between mask and aperture elements.

The cause of this fluctuation for a finite size detector is that, though the sum of path lengths through the mask material between objects A and B and the detector is always a constant value (L), during the transition between mask and aperture, this is divided between paths to objects A and B (as illustrated by the red dotted paths in Figure 43).

When a mask element completely shadows the detector, then neutrons from one of the objects are not attenuated at all and neutrons from the other are attenuated by a factor $e^{-\frac{L}{\lambda}}$ where **λ** is the effective attenuation length of the mask. Therefore, the total detected rate (R) will be:

$$R = F\varepsilon\left(1 + e^{-\frac{L}{\lambda}}\right)$$

Where F is the neutron flux incident on the detector in the absence of an attenuating mask element and ε is the detection effective area. However, during the transition, L may become divided between the two paths:

$$L = l_A + l_B$$

And the total detected rate $R_{transition}$, will be:

$$R_{transition} = F\varepsilon\left(e^{-\frac{l_A}{\lambda}} + e^{-\frac{l_B}{\lambda}}\right)$$

It can be shown that:

$R_{transition} \leq R$.

Therefore, there will be a brief drop in the total rate during these transition periods. The magnitude and duration of this effect will depend on the relative geometry of the detector and mask elements and remains an open area of research. However, the detector used in both the modeling and actual measurements was 1" in diameter and a very low Feynman-Y value was obtained. Therefore, this effect must be small for the geometry of the CONFIDANTE prototype design; at least for the counting statistics that were acquired in this work.

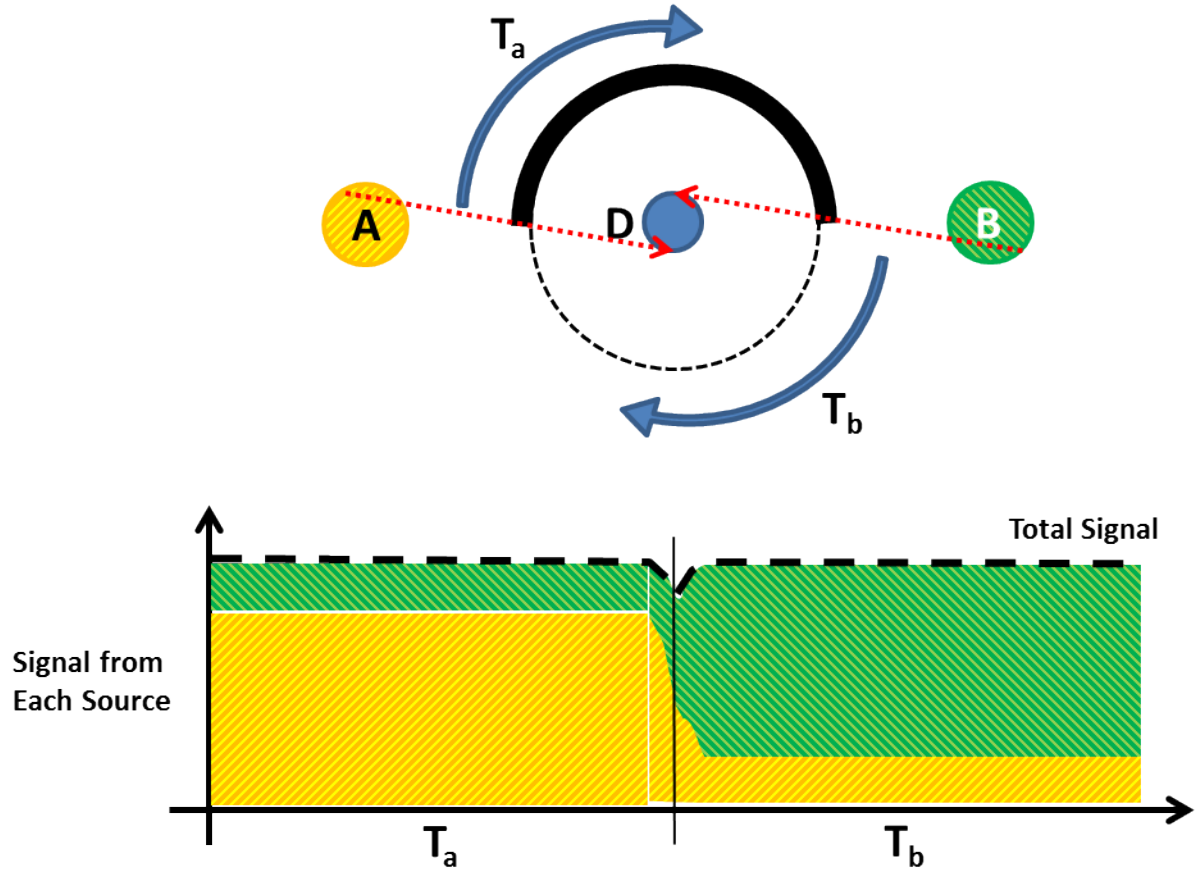


Figure 43 – (Top) Top view of an illustration of the proposed concept similar to Figure 9, but with a larger detector. (Bottom) If A and B are identical, then the sum of signals (y-axis) will be constant as a function of rotation angle (x-axis). However, during transitions between mask/aperture elements, a brief fluctuation in rate may be expected as the sum of attenuations through the edges of the mask (noted by the red dotted paths) is not equal to the attenuation through the mask.

There are couple potential avenues to mitigate this effect if it is determined to be an area of concern:

1. The ratio of the time that a mask element edge transitions the path between a source and the detector to the "flat" region can be minimized. However, this will drive the system

geometry to either a smaller detector (decreasing overall sensitivity), or larger mask elements (increasing the angular resolution).

2. If this poses an information risk too high to allow a monitoring party to handle the data directly, perhaps a metric such as the Feynman-Y could be shared instead. This would enable object confirmation without the ability to reconstruct an image. This is discussed further in the certification discussion in the following section.

6. CONCLUSIONS

We have explored several different concepts by which a Zero Knowledge Protocol might be implemented in a manner that lends more confidence in the authenticity of a confirmation measurement. In Section 2 we demonstrated that though sharing the neutron detector counts in the preloaded instrument of the ZKP implementation proposed by Glaser, Barak, and Goldston (1) could provide that confidence, it would also allow an inspecting party access to information that a host party is likely to deem sensitive. Given enough independent measurements, the underlying count distribution can be estimated even if only a subset of counts is shared in each trial. We have shown that this distribution can be used to estimate the total activity and angular size of the objects being measured.

In Section 3 we briefly explored a concept by which two simultaneous measurements could be made such that one image is subtracted from the other, eliminating the need to preload an instrument altogether. However, it was demonstrated that the variance of the difference in two count distributions contains information regarding the original count distribution. Therefore, given enough measurements (or snapshots of the same measurement) an image could be reconstructed or the intensity in certain regions of an image could be estimated. This is in addition to the practical difficulties of calibrating and matching the responses of two pixelated detector systems.

Finally in Section 4 we presented a new concept dubbed CONFIDANTE by which two treaty accountable items can be confirmed to be identical potentially without putting sensitive information at risk. If and only if the two items are identical, the fast neutron image of one item sums with the complement image of the other to a single fixed detection rate at all times within CONFIDANTE. This has several unique features that lend themselves well to both authentication and certification of a confirmation measurement:

Authentication

1. CONFIDANTE is functional as a two-dimensional imager before and after a comparison measurement without any modification to the instrument.
2. CONFIDANTE is functional as a two-dimensional imager during a comparison measurement by introducing a third source that could be provided and positioned by the monitoring party.
3. When two identical TAIs are presented, there is only a purely random count rate present in the system at all times, so the inspecting party could potentially be allowed to operate the instrument and have full access to the data.

Certification

1. When two identical TAIs are presented and well aligned, there is should not be any sensitive information at risk.
2. If the sum of the two neutron rates is a sensitive value to the host, then the host party could introduce a source with an activity unknown to the inspecting party. By placing the source directly above or below the detector pixel, its rate is unmodulated by the mask and

therefore provides a constant offset detection rate. The maximum source activity could be negotiated to prevent a strong source being used to wash out any modulation that may be present in a True Negative measurement.

3. If the host party remains concerned that sensitive information may be at risk, for example if there is worry in the alignment of the items, then the data can be further reduced to a single non-sensitive metric of how consistent the data stream is to random Poisson distributed counts. An example metric is the Feynman-Y which can be updated sequentially in relatively simple operations. For example, Figure 44 displays the sequentially updated Feynman Y value over the course of the measurement of two ^{252}Cf sources positioned 180 degrees apart. It can be seen that it has reasonably converged to a value near zero within ~100 minutes. Because there is nothing sensitive to be learned from this metric other than how random the count rate is, the inspecting party should be allowed to monitor its value.

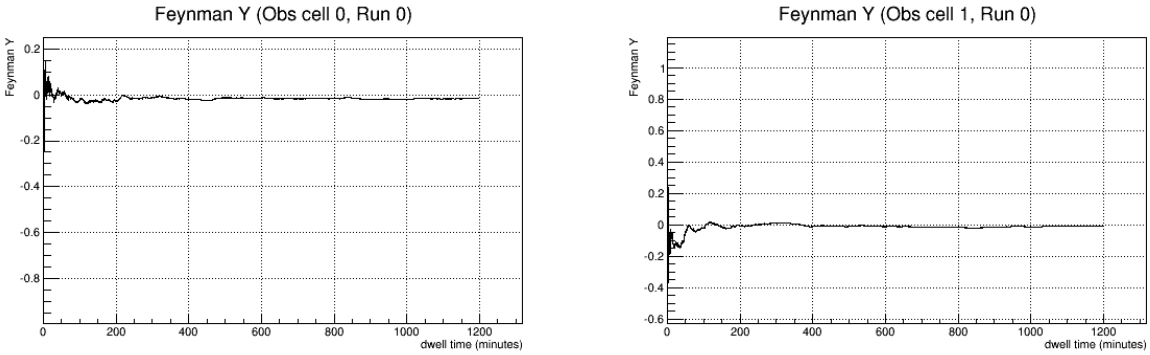


Figure 44 – Sequentially updated Feynman Y value as a function of measurement dwell time for detector pixel 0 (left) and detector pixel 1 (right) during the measurement of two ^{252}Cf sources positioned 180 degrees apart.

The success of the measurements made with the CONFIDANTE prototype system with extended volumetric distributions of SNM validate this concept as a viable option for future measurements that provide "zero knowledge" of the volumetric distribution of material while confirming that two items are identical in that distribution. Though proof of concept has been demonstrated, there remain many open research questions to explore.

7. REFERENCES

1. **Glaser, A., Barak, B., Goldston, R.** A zero-knowledge protocol for nuclear warhead verification. *Nature.* 13457, June 26, 2014, Vol. 510, pp. 497-502.
2. *Nuclear Warhead Verification: A Review of Attribute and Template Systems.* **Glaser, A., and Jie Yan.** s.l. : Taylor & Francis Group, LLC, 2015, Science & Global Security, Vol. 23, pp. 157-170. 0892-9882 print / 1547-7800 online.
3. **Dean J. Mitchell, Keith M. Tolk.** *Trusted Radiation Attribute Demonstration System.* Sandia National Laboratories. 2000.
4. *Trusted Radiation Identification System.* **K.K. Seager, et al.** Indian Wells, CA : s.n., 2001. 42nd Annual INMM Meeting.
5. *Zero Knowledge Protocol: Challenges and Opportunities.* **P. Marleau, E. Brubaker, S. Deland, N. Hilton, M. McDaniel, R. Schroeppel, K. Seager.** Palm Desert, CA : s.n., 2015. INMM Annual Meeting.
6. **P. Marleau, E. Brubaker, S. Deland, N. Hilton, M. McDaniel, R. Schroeppel, K. Seager, M.C. Stoddard, D. MacArthur.** *Report on a Zero-Knowledge Protocol Tabletop Exercise.* Sandia National Laboratories. 2015. SAN2015-5075.
7. *Fast-Neutron Coded-Aperture Imaging of Special Nuclear Material Configurations.* **P.A. Hausladen, M. A. Blackston, E. Brubaker, D.L. Chichester, P. Marleau, and R.J. Newby.** Orlando, FL : s.n., 2012. 53rd Annual Meeting of the INMM.
8. *Demonstration of Two-dimensional Time-encoded Imaging of Fast Neutrons.* **J. Brennan, E. Brubaker, M. Gerling, P. Marleau, K. McMillan, A. Nowack, N. Renard-Le Galloudec, M. Sweany.** 2015, Nuclear Instruments and Methods A.
9. *Maximum Likelihood Reconstruction for Emission Tomography.* **Vardi, L.A. Shepp and Y.** 2, October 1982, IEEE Transactions on Medical Imaging, Vols. MI-1.
10. *Outcomes of a Workshop on Techniques for Information Protection of Imaging Information.* **W.K. Pitts, E.M. Brubaker, A.J. Gilbert, N.R. Hilton, K.D. Jarman, P.A. Marleau, A. Seifert.** Atlanta, GA : s.n., 2016. INMM 57th Annual Meeting.
11. **Brubaker, E.** *Workshop on Techniques for Protection of Imaging Information: Challenge Problem.* 2016. SAND2016-4047 O.

DISTRIBUTION

1	MS0968	Rob Tachau	05753
1	MS1027	Richard Schroeppel	05635
1	MS1218	Kevin Seager	05944
1	MS1371	Diana Blair	06830
1	MS1371	Sharon Deland	06833
1	MS1371	Mike McDaniel	06832
1	MS1373	Jay Brotz	06831
1	MS1373	Gene Kallenbach	06831
1	MS1373	Heidi Smartt	06831
1	MS1373	Mary Clare Stoddard	06831
1	MS1373	Maikael Thomas	06831
1	MS1373	Tom Weber	06831
1	MS9001	Craig Tewell	08005
1	MS9004	Wen Hsu	08120
1	MS9406	Erik Brubaker	08127
1	MS9406	Nathan Hilton	08126
1	MS9406	Scott Kiff	08127
1	MS9406	Rebecca Krentz-Wee	08127
1	MS9406	Kyle Polack	08127
1	MS9406	Melinda Sweany	08127
1	MS9407	Kristin Hertz	08127
1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories