SAND2016-5714C

An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System

P. Marleau*[1] and Erik Brubaker[1]
[1]*Sandia National Laboratories*, *Livermore, CA 94551*[1]
*pmarlea@sandia.gov

Abstract

In this paper we present an authenticatable verification measurement using two-dimensional time-encoded imaging (2D-TEI) to confirm the declaration of treaty accountable items (TAIs). 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). High resolution fast neutron 2D-TEI has recently been demonstrated in proof of concept measurements of extended fission sources. We will show 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 a null result and no sensitive information must be "pre-loaded", 2D-TEI is an ideal candidate technology for Zero-Knowledge Protocols (ZKP). In recent years, the concept of 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. Last year the authors, along with several experts at Sandia National Laboratories presented an analysis of the benefits and challenges of ZKPs over more traditional warhead verification approaches. Whereas proposed physical implementations seemed to fall within the general class of template-based techniques, it was the procedural elements of ZKPs that offer many benefits. By introducing the choice between several presented objects, one of which may be a pre-authenticated reference TAI, the inspecting party gains statistical confidence that all objects are identical over many trials. However, 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. An ideal implementation of ZKP would include a comparison measurement that can be monitored during confirmation. We will show that a properly designed 2D-TEI can provide just such a measurement: because a positive is indicated by a constant rate at all times, the monitoring party can be allowed full access to the instrument before, during, and after confirmation.

[1] Sandia National Laboratories is a multi-program 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 Number 2016-XXXX

Introduction

Traditionally, verification technologies have taken one of two approaches toward confirmation of warhead authenticity: templates or attributes (1). 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 on the less sensitive attribute definition, and thus an information barrier must be implemented to protect that sensitive information used in that analysis. Several attribute measurement systems have been developed and demonstrated, though R&D in this field has declined since the late 1990s. 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 (2). 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 and 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) (3). 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 (4) (5). It was generally agreed that the physical implementations that have recently been proposed (such as (6)) 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 is off limits to the monitoring party. It is therefore detrimental to the authentication of the measurement process. The host party must preload and conduct the measurement entirely behind an information barrier leaving little confidence that an honest measurement has taken place.

The physical implementation of confirmation measurements described in this work will not require that any sensitive information be preloaded into the system. Nor will sensitive information ever be recorded; by design the neutron “images” of two TAIs exactly cancel each other out ***at all times*** if and only if they are identical; rather than only at the end of a measurement as is the case for other proposed methods. 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. Thus authentication and certification of the measurement are greatly enabled.

Two-dimensional Time-encoded Imaging: Recently, the feasibility of two-dimensional time-encoded imaging (2D-TEI) as a viable option for high resolution imaging of extended sources has been demonstrated. As shown in Figure 1, 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). The reference provided here (7) provides a more detailed description of the proof-of-concept system and the imaging concept.

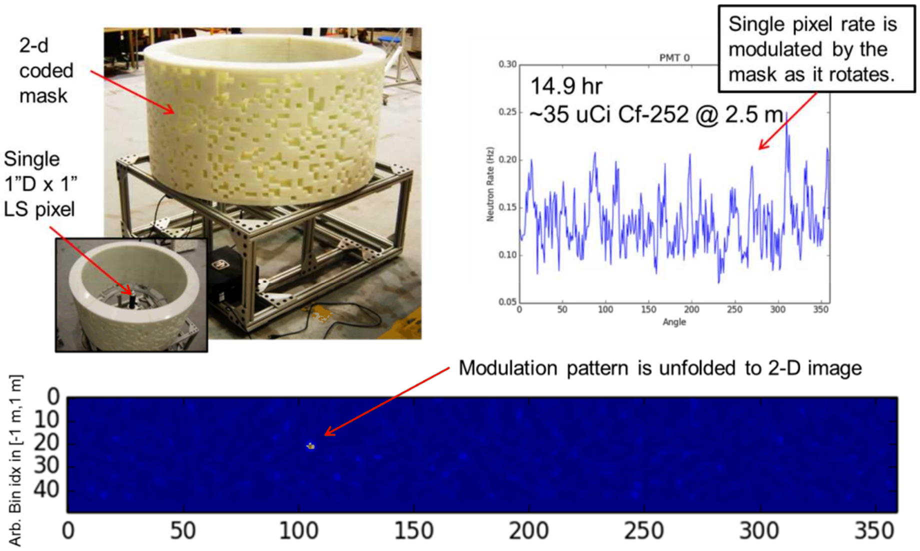

Figure 1 – The proof-of-concept time encoded imager (upper left) consists of a single 1” diameter by 1” deep liquid scintillator cell surrounded by a rotating cylindrical high density polyethylene coded mask. The modulated neutron detection rate (upper right) has the entire 2-dimensional field of view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

CONFIDANTE

CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding (CONFIDANTE) is a confirmation measurement concept based on two-dimensional time encoded imaging that removes 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.

The concept in its simplest form is illustrated in Figure 2. At the top of Figure 2 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 or aperture elements possible with the property that one half is the antimask of the other; apertures on one side are mask elements on the other and vice versa.

At the bottom of Figure 2 we illustrate a hypothetical detection rate as a function of rotation angle. When the aperture is facing object A (through region Ta), 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 Ta (where the aperture faces A) and Tb (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.

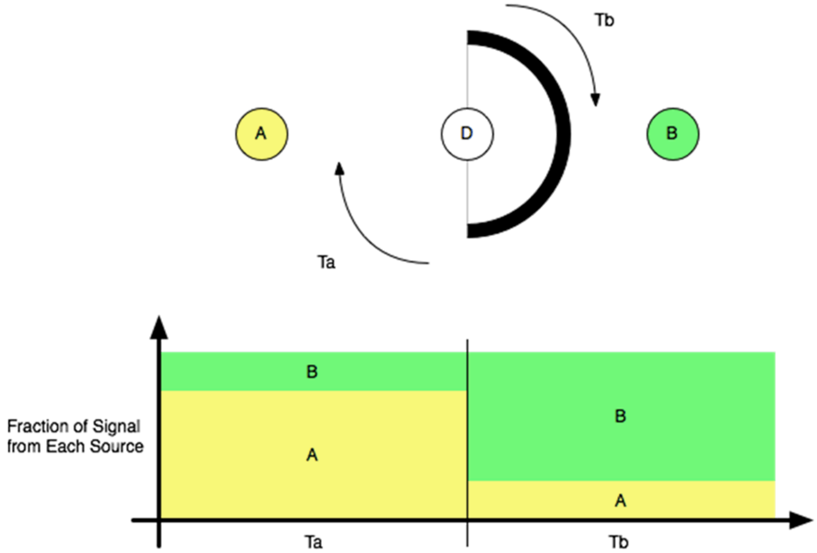

Figure 2 – (Top) Top view of an illustration of the proposed concept using the simplest example of a mask designed with one half as the anti-mask of the other. (Bottom) If A and B are identical, then the sum of signals (y-axis) will be constant as a function of rotation angle (x-axis) even though the contributions from A and B vary. Image provided by Jason Reinhardt.

In this illustration, we show a single sharp transition. This is what one would expect if A and B were point sources, but this property remains true regardless of how complicated the source's spatial distribution may be. In order to demonstrate this, we have constructed a toy model as an example. Figure 3 through Figure 6 display a progression of these results.

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 (7). A random aperture pattern with the properties discussed above was generated. Using modeling tools developed in the Time-encoded Imaging project, we then generated a detector response matrix; essentially a set of probability density functions (PDFs) for the pixel modulation as a function of rotation angle for each source bin within the field-of-view.

We then input the source distribution shown in the center panels of each figure and generated a random pixel count distribution by forward projecting through the detector response matrix and using the resultant distribution as a PDF. The resulting distributions are shown in the top, left panels and the distribution of count values from all angle bins are shown in the top, right panels. A positive confirmation of two properly positioned identical objects would be indicated by a count value distribution consistent with statistical (Poisson) noise. To illustrate this, we do two things:

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

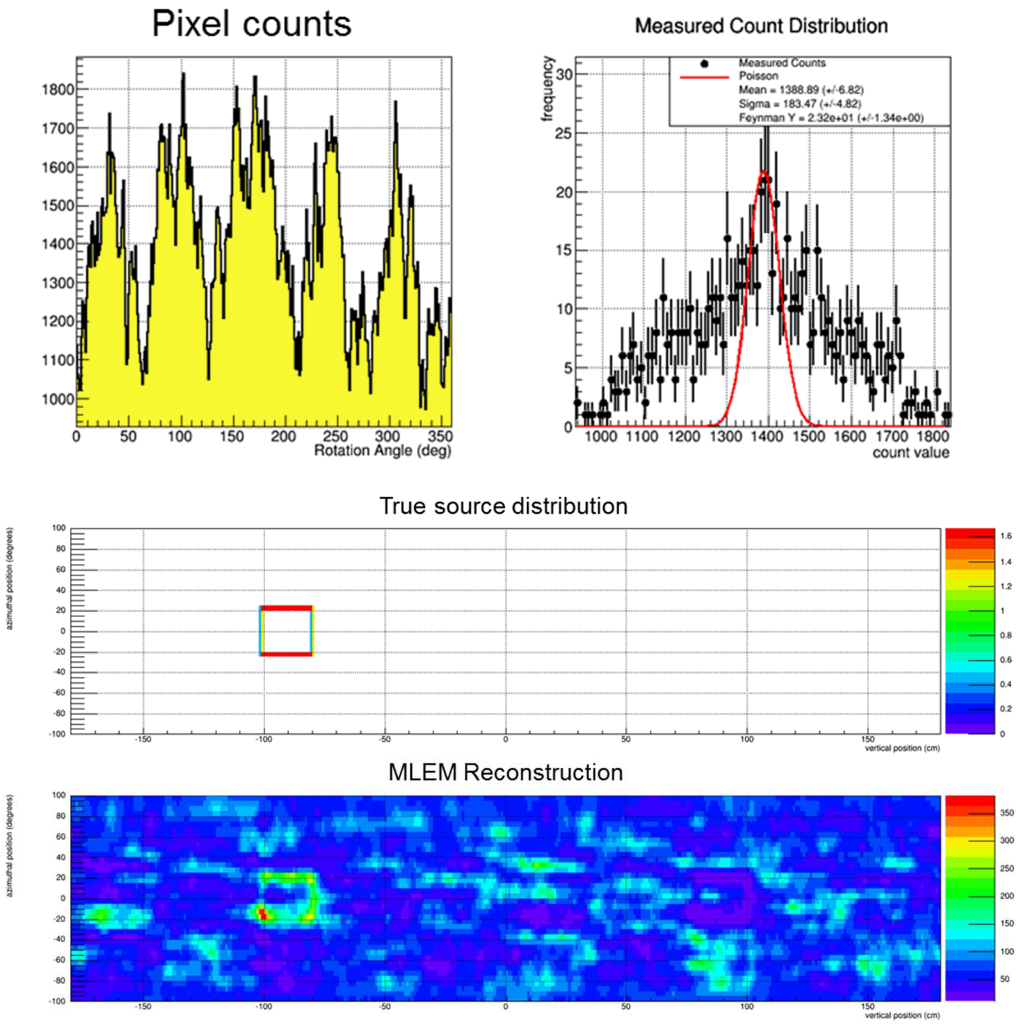

Figure 3 – Results from a simulation of a single object centered at (-90, 0). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top, left panel. The 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. A total of 1e6 events were generated. 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.

In Figure 3 we input a single object distribution. For these examples, we used a hollow-box with side dimensions (20 degrees horizontal, 40 centimeters vertical) at one meter stand-off as our TAI. It can be seen that when only a single object is present, the pixel counts demonstrate strong modulation, the count values are far from being consistent with statistical noise (Feynman Y = 23.2), 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 still capable of producing two-dimensional images.

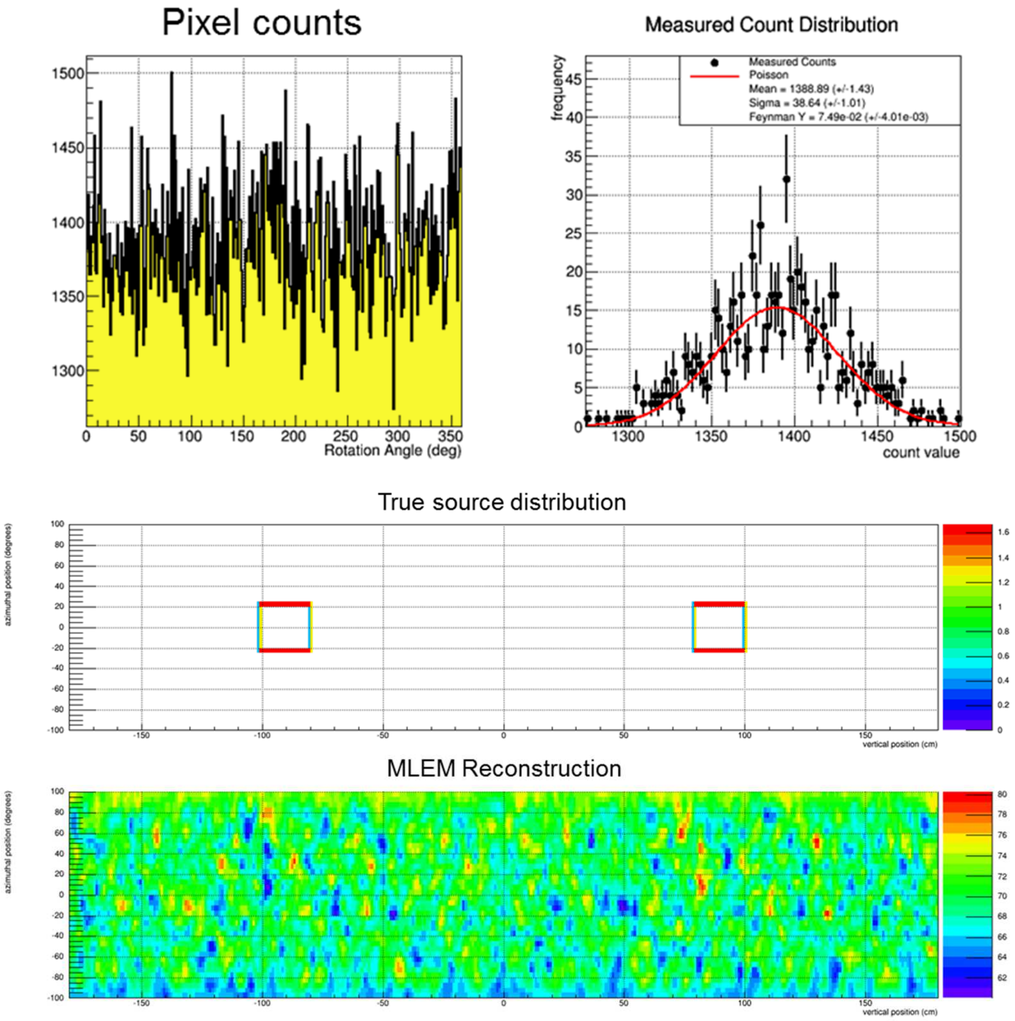

Figure 4 – Results from a simulation of a two identical objects centered at (-90, 0) and (90, 0). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top, 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. A total of 1e6 events were generated. 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.

In Figure 4 we input two identical objects positioned 180 degrees apart (on opposite sides of the system). This is the true positive confirmation test case. It can be seen visually that the count value distribution (top, right) is consistent with Poisson and the calculated Feynman Y value is 0.075. This is a small value that likely indicates confirmation; as part of the proposed work we will investigate the distribution of Feynman Y values from many trials in order to determine a threshold value that produces a low rate of false negatives. Furthermore, even if one considers the entire count distribution as a function of rotation angle (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 3 top, left) is the exact complement of the other, so their addition effectively negates the other.

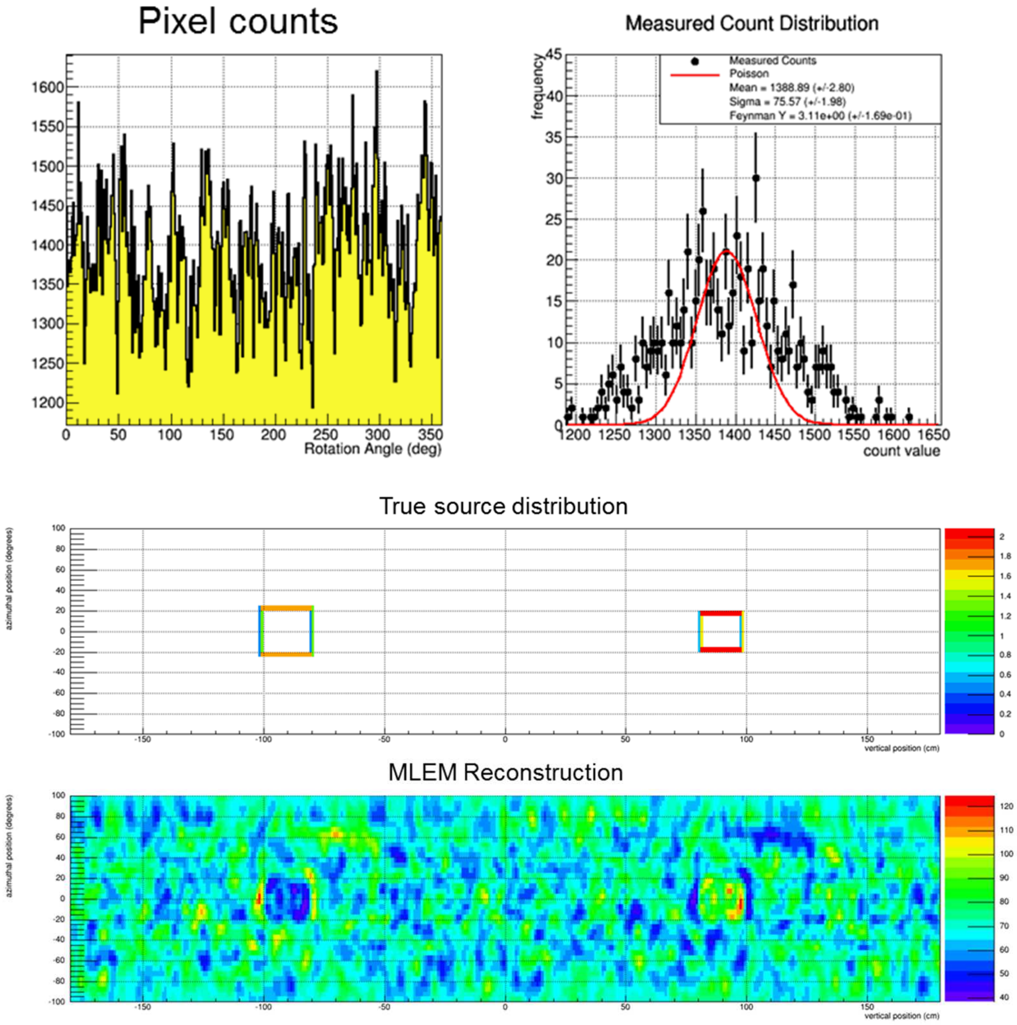

Figure 5 – Results from a simulation of a two dissimilar objects centered at (-90, 0) and (90, 0). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values for each rotation angle bin in the 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. A total of 1e6 events were generated. 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.

In Figure 5 we input two objects; however one is inconsistent with our definition of TAI. Again, it can be seen that the count value distribution (top, right) is not consistent with being Poisson (Feynman Y = 3.1). Additionally, if the count distribution as a function of rotation angle (top, left) is used to reconstruct an image (bottom), a combination of both objects is apparent. 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 better lending itself to authentication measures.

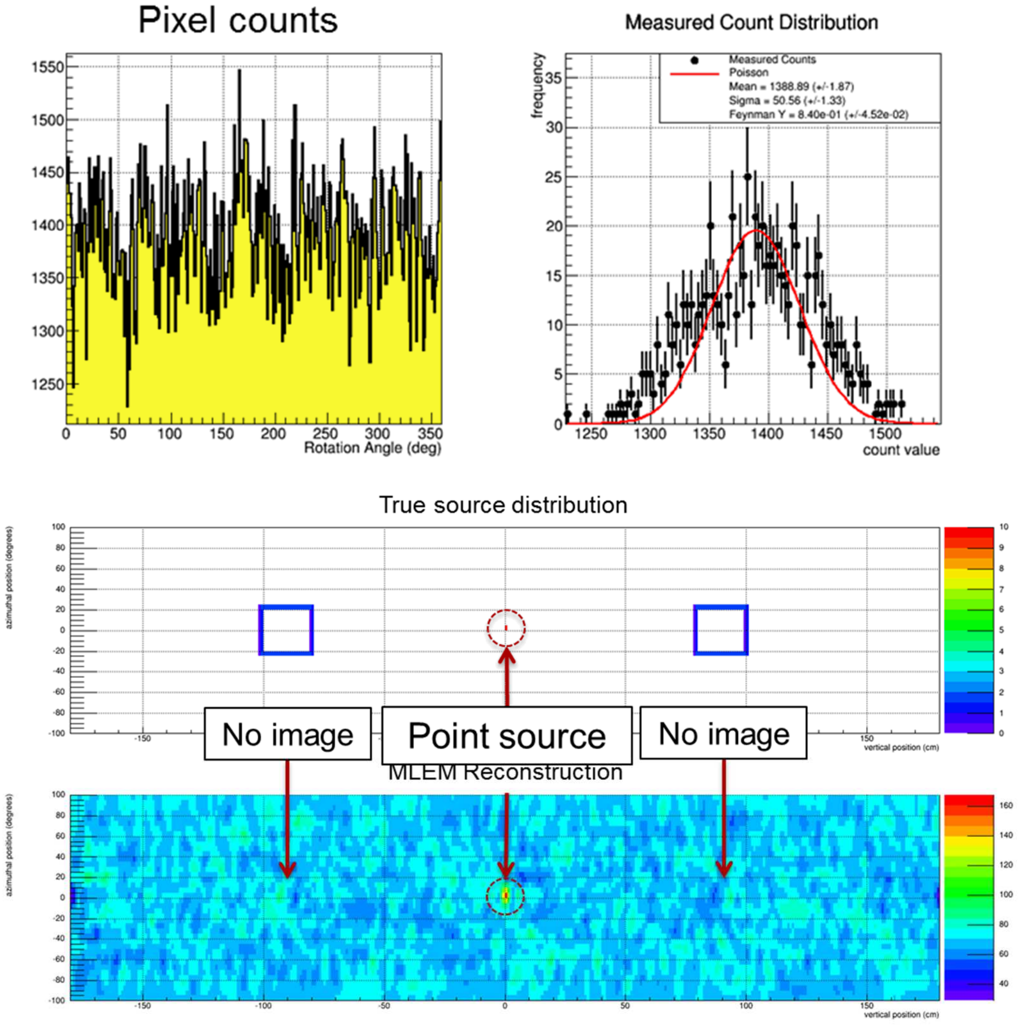

Figure 6 – Results from a simulation of a two identical objects centered at (-90, 0) and (90, 0) and a single point source at (0, 0). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values 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. A total of 1e6 events were generated. 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.

Finally, in Figure 6 we input two identical objects that should produce a true positive and add an additional point source. This is to demonstrate that, even as the two identical objects cancel each other out, the system is still functional as an imager. This may open up measurement authentication procedures such as allowing the monitoring party to bring a source to be imaged during the confirmation measurement. Such a measure would lend strong confidence that the equipment is functional and a measurement is taking place.

Conclusions

We have presented a new concept useful for the confirmation that two treaty accountable items are identical without putting sensitive information at risk. If and only if two items are identical, the fast neutron image of one exactly sums to a single fixed detection rate with the fast neutron anti-image of the other at all times within CONFIDANTE. This has several unique features that lend themselves well to both authentication and certification:

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 no sensitive information at risk, so the monitoring party could be allowed to operate the instrument and have full access to the data.

Certification

1. When two identical TAIs are presented, there is no 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 monitoring 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 the items are not perfectly aligned, then the data can be further reduced to a single non-sensitive metric of how consistent the data stream is to pure Poisson noise. An example metric is the Feynman-Y which can be updated sequentially in relatively simple operations. This could be implemented in a simple ASIC and does not require the use of a digital computer or software.

A proof-of-concept prototype of CONFIDANTE is currently being constructed (shown in Figure 7) and we expect that the results of laboratory measurements using two-matched neutron sources will demonstrate the feasibility of this concept.

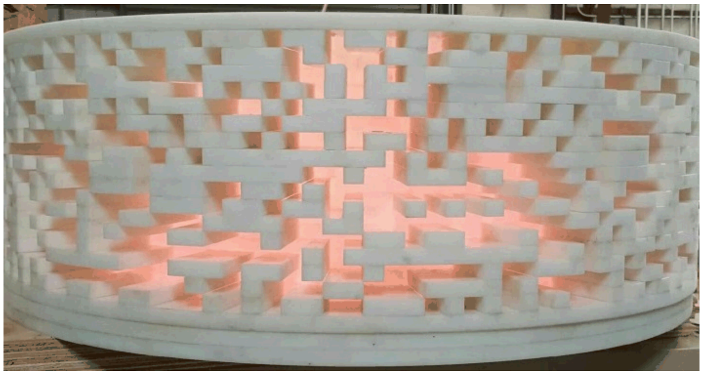

Figure 7 – The proof-of-concept CONFIDANTE prototype.

Acknowledgements

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

References

1. **Spears, D.** *Technology R&D for Arms Control.* Arms Control and Nonproliferation Technologies, Office of Nonproliferation Research and Engineering. 2001.

2. **Tolk, Dean J. Mitchell and Keith M.** *Trusted Radiation Attribute Demonstration System.* Sandia National Laboratories. 2000.

3. *Trusted Radiation Identification System.* **K.K. Seager, et al.** Indian Wells, CA : s.n., 2001. 42nd Annual INMM Meeting.

4. *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.

5. **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.

6. **Glaser, A., Barak, B., Goldston, R.** A zero-knowledge protocol for nuclear warhead verification. *Nature.* 13457, June 26, 2014, Vol. 510, pp. 497-502.

7. *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.