nature COMMUNICATIONS

ARTICLE

https://doi.org/10.1038/s41467-019-12386-0 OPEN

A physically cryptographic warhead verification system using neutron induced nuclear resonances

Ezra M. Engel[1] & Areg Danagoulian[1*]

Arms control treaties are necessary to reduce the large stockpiles of the nuclear weapons that constitute one of the biggest dangers to the world. However, an impactful treaty hinges on effective inspection exercises to verify the participants' compliance to the treaty terms. Such procedures would require verification of the authenticity of a warhead undergoing dismantlement. Previously proposed solutions lacked the combination of isotopic sensitivity and information security. Here we present the experimental feasibility proof of a technique that uses neutron induced nuclear resonances and is sensitive to the combination of isotopics and geometry. The information is physically encrypted to prevent the leakage of sensitive information. Our approach can significantly increase the trustworthiness of future arms control treaties while expanding their scope to include the verified dismantlement of nuclear warheads themselves.

[1] Department of Nuclear Science and Engineering, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA. *email: aregjan@mit.edu

As of 2019, there are estimated 13,000 nuclear weapons that make up the nuclear arsenals of the United States and Russia[1,2]. Such large arsenals may be one of the greatest threats to our civilization. While high, these numbers are a significant reduction from the Cold War era, as a result of series of arms control treaties. The past treaties between United States of America and Soviet Union/Russia, however, primarily focused on the verified dismantlement of the delivery systems, such as ballistic missiles and strategic bomber aircraft. This circumstance in part was driven by the notion that the delivery systems can be a good proxy for the states' strike capability during a nuclear war. It was also driven by the difficulty of verifiably dismantling the warheads themselves without leaking sensitive information about the weapon designs in the process[3]. This approach has left behind large stockpiles of surplus nuclear weapons, exposing them to the risk of theft and unauthorized or accidental use, as well as transfer to third countries. This state of the affairs elevates the risk of nuclear terrorism and nuclear proliferation. The need for more effective arms control treaties is recognized by the 2018 US Nuclear Posture Review, which noted that "The United States will continue its efforts to seek arms control agreements that enhance security, and are verifiable and enforceable"[4]. Furthermore, there are increased worries that unless new treaties are implemented the current arsenal sizes will stagnate at the current numbers[2,5]. New treaties involving the verified dismantlement of nuclear warheads will significantly improve global security. However, new types of technologies are necessary to enable such treaties. These technologies will have to detect hoaxing attempts, clear honest warheads as such, while simultaneously protecting sensitive information about the weapon designs.

A variety of paradigms of verification have been proposed by a number of scholars and scientists. The most recent of these, the template verification paradigm, is based on the expectation that the inspection party will be able to acquire an authentic device (henceforth referred to as the genuine reference object) and then use relevant encrypted data (known as a template) from this device to compare with equivalent data acquired from candidate devices of the same design. The key to this verification process is a proof system that can guarantee that no treaty accountable item (TAI) undergoing verified dismantlement is secretly modified. A number of works have been published on the philosophy behind this template verification—in the US national laboratories, think tanks, and academia[6–8]—and a variety of concepts have been proposed[8–16]. Common to all these studies is the concept of the genuine reference object, which is acquired based on a situational context and brought to the testing facility via a chain of custody. For a more detailed delineation of the procedure describing the acquisition of the genuine reference object (sometimes referred to as golden copy in the literature) and its use in the verification exercises, see "Results" section in our previous work, Hecla and Danagoulian[17]. That work as well as the one presented in this study leverage Neutron Resonance Transmission Analysis (NRTA). This technique uses neutron-induced nuclear resonances in the electron-Volt (eV) energy range, common in many high Z elements, including molybdenum, tungsten, uranium, and plutonium, to achieve high-resolution imaging of the individual isotopes of those elements[18]. The strength of NRTA stems from the uniqueness of the resonance energies and amplitudes to individual isotopes, thus making their observation a unique tag of a particular isotope's abundance in the sample. NRTA has been previously used to image and study various nuclear fuel samples and archaeological objects—for an in-depth discussion, see Losko et al. and Bourke et al.[19,20].

Some of the previously proposed concepts made use of physical cryptography. This has the advantage of avoiding computational cryptography, which can be prone to hacks and backdoor exploits and as such shifts the burden of verification to the computer code and electronic components. Work by Philippe et al.[11] had the advantage of achieving the highest level of information security via a zero-knowledge measurement, yet it is not fully sensitive to isotopic hoaxes due to the similarity of fast neutron processes between various nuclei. Additional work is currently underway to mitigate this circumstance, e.g., by observing fast neutrons from neutron-induced fission[21]. Others, such as those by Vavrek et al.[16], leverage nuclear resonance phenomena to achieve strong isotopic sensitivity to hoaxes but do not have zero-knowledge information security and involve complex systems that may be unpractical in a verification setting. Our previous study, Hecla and Danagoulian[17], was based on Monte Carlo (MC) simulations, where we combined the advantages of a neutron-based radiographic system with the isotopic sensitivity of a nuclear resonance-sensitive measurement to achieve an effectively zero-knowledge proof system.

In this paper, we build upon the general concepts described previously by Hecla and Danagoulian[17], with important differences and modifications. The study by Hecla and Danagoulian was based on MC simulations alone and envisioned an imaging system where the physical encryption is achieved by a geometrically complex reciprocal mask. The concept proposed in this work meanwhile achieves an experimental feasibility proof of concept involving a simple encrypting filter and uses a single-pixel neutron detector. The detector measures the combined flux through the object and can determine the energy of individual neutrons. While a single-pixel measurement along one axis of measurement does not have geometric uniqueness, such a uniqueness can be achieved via multiple measurements with object rotations, not dissimilar to the principles of a tomographic system. This requires a new procedure for the comparisons between template data from the genuine reference object and the equivalent data from the candidate items. This study's advantage is in the simplicity of the measurement as it avoids actual imaging and thus enables higher degree of information security. It is also a direct experimental proof of feasibility, which is sensitive to the backgrounds, noise, and system instabilities not captured in a numerical simulation.

Results

Template verification. The overall high-level verification exercise is described in detail in the "Results" section of Hecla and Danagoulian[17]. In brief, in an unannounced visit to an ICBM base the joint team of the inspectors and the hosts acquires a randomly selected nuclear weapon, whose authenticity is thus established by its situational context. The weapon is then transported under joint custody, i.e., in the presence of both parties and via application of tamper-proof seals and checks[22], to a facility where it is disassembled in a controlled environment such that no new objects are introduced or removed. The fissile hollow sphere, from here on referred to as the pit, is removed and used as a genuine reference object. This study focuses on the stage involving the actual measurements test, where the genuine reference object is being compared to the TAI candidate objects. The test needs to detect both isotopic hoaxes as well as geometric hoaxes, described later in this section. The experimental procedure consists of the following steps:

1. The genuine object, an encrypting filter, and the neutron detector are aligned along the beam z axis. The encrypting filter is produced by the host, and its composition is unknown to the inspectors. The system schematic can be seen in Fig. 1. The filter can be made of any material, with the assumption but not the requirement that the hosts will add elements identical to those in the TAI, with the only

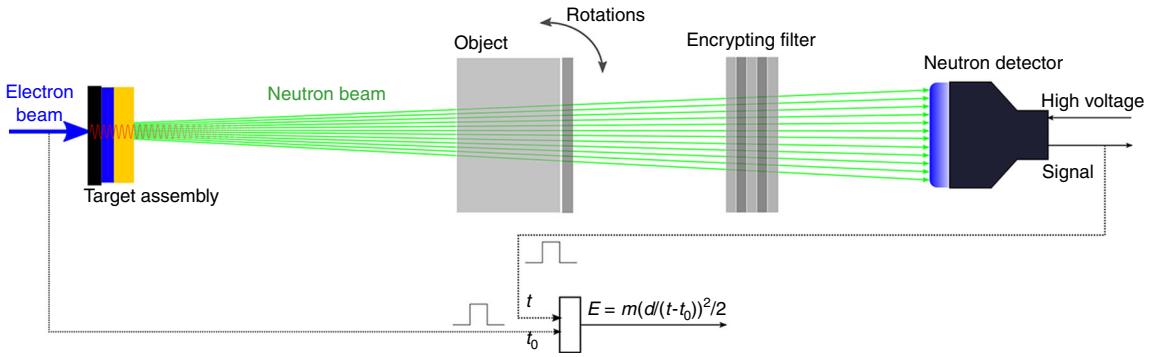

Fig. 1 General schematic of the experiment (not to scale). The combination of isotopic and geometric sensitivity is achieved by neutron spectroscopy via time-of-flight (TOF) technique and comparisons between the candidate and the genuine reference under random projections. For simplicity, in this experiment the angles of the projections were chosen to be 0, 45°, and 90°

requirement being that the filter allow a significant flux of neutrons to reach the detector for an agreed upon measurement time. A spectroscopic measurement is taken, providing the template data (from here on referred to as template) that the next measurements will be compared to.
2. Keeping the encrypting filter and the detector in their places, the genuine object is replaced with the candidate object at the same orientation. A measurement under experimental conditions identical to step (1) is performed.
3. The data from the measurement of the candidate object is compared with the template in a statistical test. If the test identifies a statistically significant difference, then the candidate is declared a hoax. If the new measurement passes the statistical test, then the procedure moves on to the next stage, where measurements under random rotations are performed.
4. Measurements described in the steps (1) and (2) are now repeated with both genuine and candidate objects rotated at a random angle. To keep the number of unknowns larger than the number of measurements, a new encrypting filter is provided by the hosts. Like before, the filter is kept in place during the two (genuine, candidate) rotated measurements. Similar to step (3), the two measurements are compared in a statistical test. If the measurements pass the statistical comparison, then the candidate is declared isotopically and geometrically identical to the genuine and is thus accepted as genuine as well.

This work focuses on a sensitivity study, experimentally demonstrating the feasibility of the comparison. The technique is shown capable of clearing objects identical to the genuine reference object and rejecting objects that are isotopically or geometrically different. The verification exercise focuses on the weapons-grade plutonium (WGPu) pit, primarily due to the weapon's hydrogenous components' near-opacity to epithermal neutrons. HMX explosive, for example, has a mean free path of ~1.8 cm for epithermal neutrons. Public domain data on estimates of a Soviet thermonuclear design[23] indicate that the explosive's thickness can be ~6.5 cm, translating to an attenuation factor of about 1000. While not impossible, a transmission measurement of weapons at a lesser degree of disassembly would require either more intense neutron sources or longer measurement times. This may become possible in the future, as the laser-driven and other high-intensity neutron sources currently under development become more applicable for field use[24,25]. It should be added that the plutonium pit may also contain other materials, such as coatings, to prevent the air's corrosive effects on plutonium, as well as the beryllium neutron reflector shell, which may be bonded to the plutonium shell. The latter has a mean free path of 1.3 cm for eV neutrons, and depending on its thickness its attenuation effects may translate to measurement times somewhat longer than those estimated in this work. This study thus focuses on an inspection scenario where the plutonium pit has been extracted in a controlled environment and undergoes verification, as described in prior work[17].

The experiment. The overall diagram of the measurement set-up can be seen in Fig. 1 and is discussed in more detail in the "Methods" section. The neutrons are produced in a pulsed mode from a pulsed electron linear accelerator, via a tantalum bremsstrahlung–photoneutron converter, which produces neutrons via the (γ, n) reaction. A 2.54 cm polyethylene moderator degrades the neutrons' energy from the ~MeV scale to the ~eV scale. As the epithermal neutrons traverse the object and the encrypting filter, their spectrum is modulated in accordance to the cross-sections and areal densities of the relevant isotopes, after which they are detected by a ^{6}Li glass scintillator detector. The detector produces a timing pulse, which is compared to the timing pulse of the linear accelerator. This comparison allows to determine $t_{\mathrm{tof}} = t - t_0$ of the neutrons. The energy of individual neutrons can then be reconstructed via $E = m(d/t_{\mathrm{tof}})^2/2$, where m and d are the neutron mass and the flight path length, respectively. The transmission spectra are normalized to the incident neutron count, determined by a fission chamber (not shown) upstream of the target object.

Targets. As the research was performed in academic setting, plutonium and uranium targets were not available. Thus targets were built of more commonly available materials that have significant resonances in the relevant region of $1\ \mathrm{eV} \le E \le 200\ \mathrm{eV}$ and can thus act as proxies for most uranium or plutonium isotopes. Natural molybdenum and tungsten were chosen as element-to-isotope proxies for ^{239}Pu and ^{240}Pu, respectively. Instead of hollow spheres, which are typical to nuclear weapon pits, simpler cylindrical geometries were chosen, such that the genuine proxy object is a cylinder of 50.8 mm diameter and 30 mm length, with the first 27 mm consisting of molybdenum and 3 mm consisting of tungsten. Such a combination was chosen to mimic the ~90% enrichment of WGPu. Plots of total neutron interaction cross-sections for a subset of molybdenum and tungsten isotopes can be seen in Fig. 2. Unlike molybdenum or tungsten, the actinide targets would produce additional neutrons via the $(n, \mathrm{fission})$ reaction. However the resulting neutrons would be of the ~MeV energies, making the ^{6}Li detector insensitive to them. The encrypting filters were assembled from 3 mm and 6.35 mm thick tungsten and molybdenum plates, respectively, that had 76.2 mm × 76.2 mm outer dimensions. The

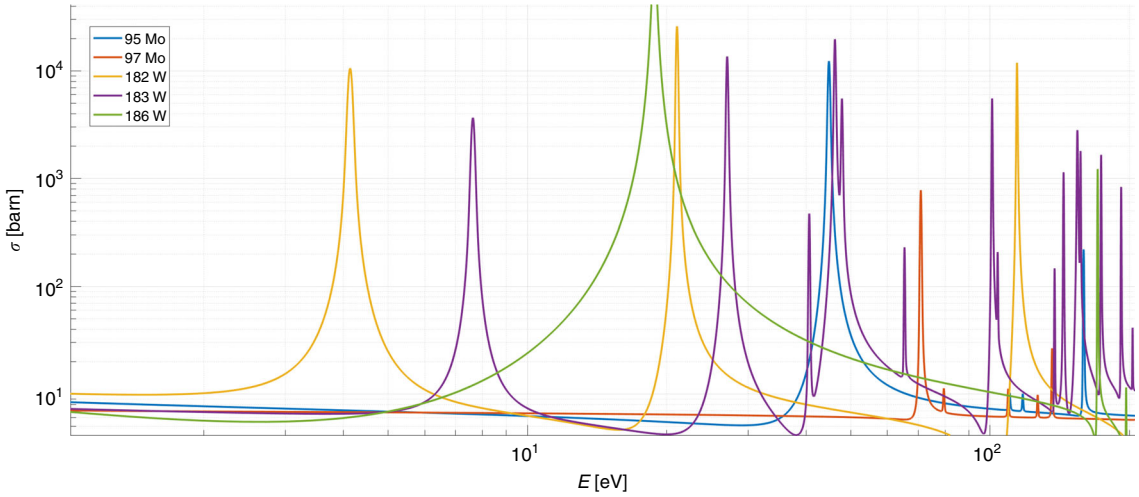

Fig. 2 Cross-sections. Total interaction cross-sections for neutron-induced interactions for a subset of molybdenum and tungsten isotopes with significant resonances in the 1–200 eV range

measurements at 0° rotation, described in Figs. 3, 4a, and 5a, used a filter consisting of three tungsten and three molybdenum plates aligned with the beam. The measurements at 45° used a filter consisting of two tungsten and one molybdenum plates, and at 90°, the filter consisted of one tungsten and one molybdenum plates. See "Methods" for additional detail on experimental settings.

Epithermal neutrons. In this experiment, the neutron energies at the source spanned from the ~MeV scale, known as fast neutrons, to ~meV, referred to as thermal neutrons. However, the use of a thin cadmium filter near the source filtered out most neutrons <0.5 eV. The detector used to register the neutron hits was based on ^{6}Li isotope, which interacts with neutrons via the ^{6}Li(n, t)α reaction, with the triton and the alpha causing scintillation in the glass and thus triggering detection. When combined with the time-of-flight (TOF) technique, this allows to determine the neutron's kinetic energy with ≪eV precision, allowing to resolve narrow absorption lines such as the 0.13 eV wide line at 70.9 eV from ^{97}Mo. The spectra in Figs. 3–5 were produced via this method.

The results of isotope-specific resonant absorption are most readily observable in Fig. 5. The solid vertical gray lines indicate the expected positions of the tungsten resonances, while the dotted lines indicate the positions of the molybdenum resonances. Depending on an isotope, the resonances are due to the (n, γ) and (n, n') reactions, which selectively remove neutrons from the beam at the resonant energies. The relative depth of the absorption lines primarily depend on the resonance width, with broader widths translating to higher integrated cross-sections and thus more absorption. The shape of the absorption line in part depends on the type of the interaction. These combined absorption features yield a unique spectral fingerprint of a particular configuration of isotopic, geometric, and density distribution. Future research, however, should focus on providing a systematic proof of this uniqueness, i.e., that no combination of other elements can reproduce uranium or plutonium signatures. See Supplementary Note 4 for a detailed discussion.

Isotopic hoax resistance. Isotopic hoax resistance refers to a system's ability to detect hoaxing attempts, which involve modifications of the isotopic ratios in an otherwise geometrically identical object. For a real warhead, this may involve replacing the WGPu pit, which has enrichment levels of >90%, with a pit made from the more available reactor-grade plutonium (RGPu), which has a lowered ^{239}Pu enrichment of approximately 60%, with the remaining ~40% in the form of ^{240}Pu.

To test the sensitivity of the technique to isotopic variations, the 90%:10% Mo:W genuine reference object's transmission spectrum was compared to the transmission spectra of 50%:50% and 10%:90% Mo:W objects of the same cylindrical shape and overall dimensions. Figure 3 shows the plots and comparisons of the spectra. The comparisons show that, as the proportion of tungsten is increased, the tungsten absorption lines show increased absorption, while the molybdenum lines exhibit reduced absorption, as expected. A simple χ^2 test can be applied, determining the values of χ^2 and the corresponding probability p that the difference is merely due to random fluctuations. For these comparisons, the p value is consistent with zero to ten significant digits and thus indicates that a systematic difference is present. The χ^2 test thus rejects the comparison and indicates a hoaxing attempt. All measurements lasted approximately 5 min.

Geometric hoax resistance. A single measurement along the beam's z axis is only sensitive to the projected isotopics along that axis. The transmission T for an energy bin E and a spherically symmetric geometry can be approximated as

$$\ln T \simeq -2\pi N_{\mathrm{Av}} \sum_i \frac{\sigma_i(E)\rho_i}{A_i} \int_1^{\cos\theta'} \int_0^X f_i(r, \cos\theta) \mathrm{d}r \mathrm{d}\cos\theta,$$

where $\sigma_i(E)$, ρ_i, X, θ', and A_i are the cross-section, density, total thickness, polar angle, and atomic number for isotope layer i of the object, respectively. $f_i(r, \cos\theta)$ is the fractional abundance of isotope i at a particular radial coordinate, and N_{Av} is Avogadro's number. The summation takes place over all the isotopes, and the integration is along the radius and the polar angle. Thus the single-pixel camera measurement effectively collapses the three dimensions into a zero-dimensional energy-dependent-only measurement. This limitation can be readily overcome by making multiple measurements at various angles, similar to tomographic measurements where a single pixel can ultimately produce a three-dimensional sensitivity. Unlike a tomography where the goal is to produce a three-dimensional image, here the goal is to simply verify that two objects are identical to within some level of geometric complexity. Prior work has shown that two to three measurements at randomly selected angles are sufficient to achieve this goal[12]. The random selection of the angles

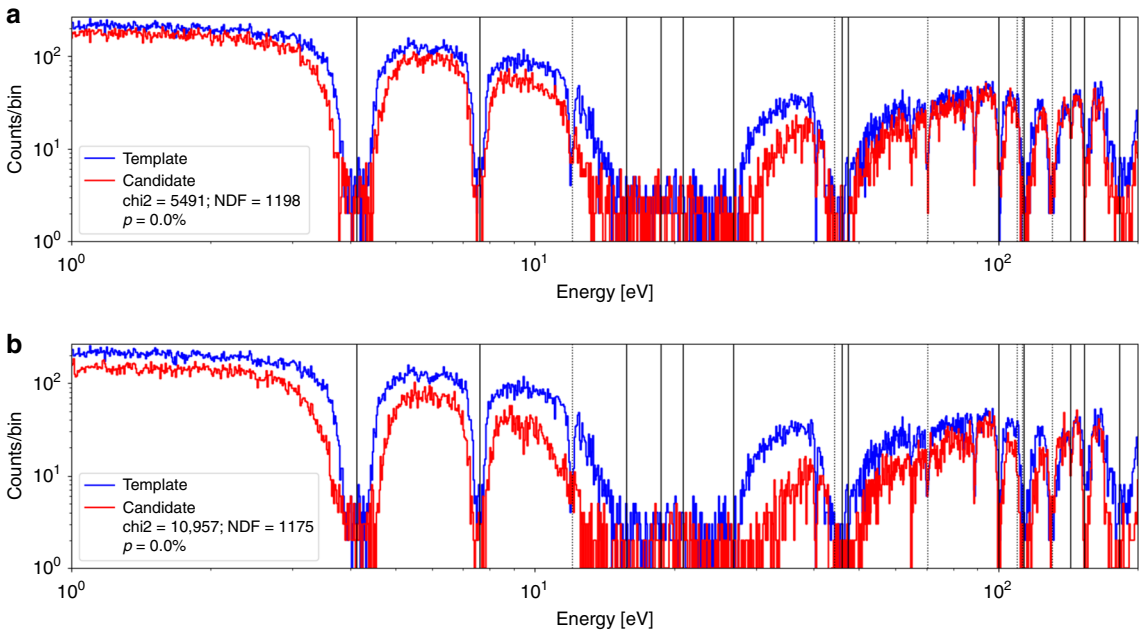

Fig. 3 Histograms of neutron count energies for two isotopic hoaxes. **a** The template data from an authentic reference of 90/10 Mo/W composition (blue) is compared to the data from a 50/50 Mo/W isotopic hoax (red). **b** The data from the authentic reference is compared to that from a 10/90 Mo/W isotopic hoax (red). The legend lists the χ^2 value, the number of degrees of freedom, and the corresponding probability (p value) for the χ^2 test. Both hoaxes are rejected. The solid and dashed vertical lines denote the locations of some of the known tungsten and molybdenum resonances, respectively. Data collection lasted approximately 5 min per object

at the time of the verification exercise renders the hosts unable to optimize a possible geometric hoax to the measurement. The problem is thus reduced to proving that the system is sensitive to geometric differences under rotations.

To show this sensitivity, we perform measurements at 45° and 90° relative to the beam's z axis. For this purpose, the geometric hoax object was chosen to be a rectangular parallelepiped, i.e., a box, of the same composition along the z axis as the genuine reference object. It consists of a $50.8 \times 50.8 \times 27$ mm^3 box of molybdenum followed by a $50.8 \times 50.8 \times 3$ mm^3 plate of tungsten. Since the beam diameter is only 44.5 mm, the spectral measurement results from two objects should look identical at 0°. However, at 45° and 90°, the geometric differences should amount to different values of ln T.

To test the above hypothesis and the sensitivity of the system under rotations, the measurements were performed under identical beam conditions. Furthermore, for every rotation the encrypting mask was modified but kept the same between genuine and candidate comparisons. This is a necessary step, in order to prevent any differential analysis of data from multiple angles, which may otherwise reveal geometric information. In analogy to an under-defined system, every new measurement needs an additional unknown, in the form of a different encrypting filter. Figure 4 shows the spectral comparisons. It can be seen that at 0° the spectra are essentially identical, when compared with a χ^2 test. However, when rotated the small but significant differences in geometries give rise to detectable deviations. While not as large as in the isotopic hoax, the differences are nevertheless statistically significant. This result shows that, for these experimental settings, object types, and measurement times, the system can detect these geometric hoaxes with rotations by $\theta \geq 45°$.

In this experiment, all the rotations were centered on the geometric center of the object. However, hollow spheres of the same thickness but different radii would produce identical signals under such rotations, due to their spherical symmetry. This would result in an effective geometric hoax. To break this symmetry, the rotations should either involve a randomly chosen center or be followed by random translations. Overall, this study focuses on a limited set of hoaxing scenarios, and future studies need to focus on further extending these tests. As with most cryptographic protocols, the concept presented in this work should undergo future tests and checks. The use of the K-transforms in particular may prove promising in providing a proof of geometric uniqueness[12].

Completeness. Finally, the test procedure needs to also show that it is able to accept honest candidates. As with the geometric hoax sensitivity test, here the test needs to clear the honest candidates at 0°, 45°, and 90° rotations, as a way of confirming that the objects are identical both isotopically and geometrically. We thus repeat the procedure described in the previous subsection. This is necessary in order to rule out the possibility that the previously observed differences were merely the results of system instabilities, such as beam energy variations or detector gain shifts. Figure 5 shows comparisons where the genuine reference object measurements are compared to those from identical, honest objects. Between these measurements, the honest objects as well as the encrypting filters were replaced with other targets and filters and then were placed back for the comparison measurements. A marker on the target holder allowed for the precise setting of the rotational angle. In one case, the accelerator had to be turned off and restarted owing to beam instabilities. As expected, and despite technical disruptions, in all cases the χ^2 test indicates that the differences are merely statistical, as the p value of the test indicates an agreement. It is then concluded that the system is capable of clearing honest candidate objects. A summary of the test results are listed in Table 1. Per procedure described at the beginning of the section, the test immediately rejects the attempts at isotopic hoaxing. The geometric hoax shows an identical signal to the genuine reference object at

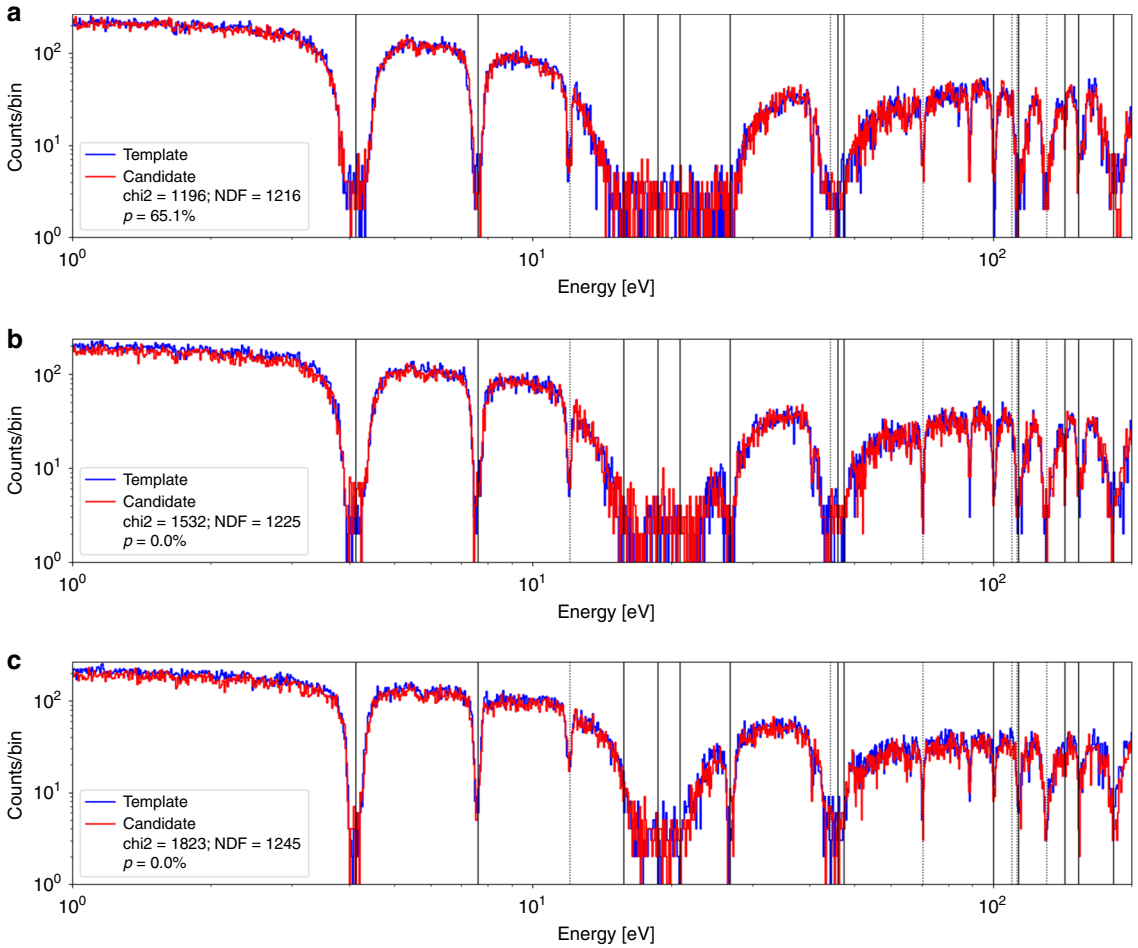

Fig. 4 Histograms of neutron count energies for a geometric hoax. The geometric hoax has been constructed as to have the same areal density along z axis as the genuine reference. The template data from a genuine reference (blue) is compared to the data from the geometric hoax (red) at $\theta = 0°$ (**a**), $\theta = 45°$ (**b**), and $\theta = 90°$ (**c**). As expected per design, $\theta = 0°$ yields a perfect agreement, as shown by the p value. The rotations readily expose the hoax

measurements along the z axis; however, rotations by ≥45° immediately results in a rejection. Finally, the honest candidate measurements pass the test for all angles of rotation and are thus accepted as honest objects.

It is necessary to acknowledge that a small rate of false positives may be caused by difference in ages between honest pits, caused by slight differences in ^{241}Pu concentrations due its beta decay into ^{241}Am, as well as machining tolerances in pit production. As demonstrated in Supplementary Note 3, the former is a minor effect that should not cause false positives for pits with age difference of <10 years. The latter effect can be accurately estimated only given classified information on pit production and should be addressed in the classified setting. Our current modeling indicates that differences of <1 mm should not trigger false positives.

Information security. One of the important goals of the verification system is the information security, that is, the inspectors' inability to learn significant information about the TAI. In our prior work, we showed via computational simulations that while the inspectors can learn information about the combined content of the TAI and the encrypting filter, they cannot learn anything specific to the TAI itself—see Hecla and Danagoulian[17], subsection on Isotopic Information Security. The primary focus of this study is the sensitivity analysis, with the purpose of showing that the concept is capable of detecting hoaxing attempts. Nevertheless, we use experimental data from the measurements in combination with a Geant4[26,27] computational model of the experiment to simulate scenarios with a WGPu pit and an encrypting filter of WGPu weighting 1.8 kg. In these data-driven simulations, we show that various opposite combinations of the TAI and filter geometries produce statistically indistinguishable signals. This makes it impossible for the inspectors to learn information of value, similar (but not identical) to the concept of zero-knowledge proof. At the same time, additional simulations show that pairs of 5 min-long measurements at an experimental facility similar to the one used in this study can readily detect cheating scenarios where the WGPu pit has been replaced with RGPu or where its size has been reduced by ≤2 mm, depending on experimental conditions. See Supplementary Note 3 for a detailed discussion. In Supplementary Note 1, it is demonstrated that using an encrypting filter of just 1.8 kg will result in an inferred range of pit's possible mass that spans from zero to a value that is significantly larger than the critical mass. At the same time, the combined target thickness will be small enough to allow for significant counting statistics and thus reasonable measurement times. The impact of temperature-dependent broadening of the resonances is also estimated and described in Supplementary Note 2, showing that the effect can be made negligible.

The presence of absorption lines associated with weapon materials whose presence may be a priori unknown to the inspecting side is an important consideration in the context of information security. If those materials were to have resonances in the energy domain of the measurement, the inspector would

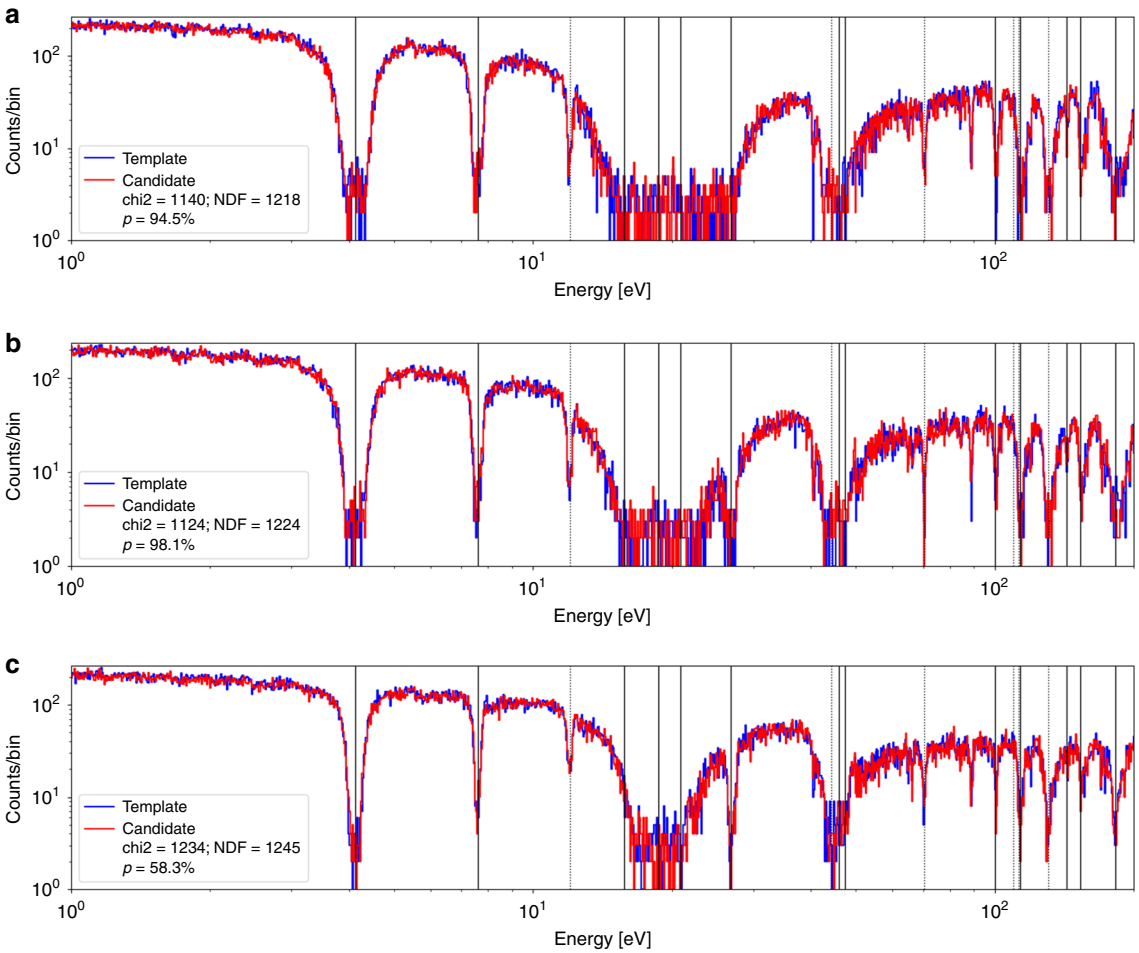

Fig. 5 Spectral comparisons between a genuine reference and an honest candidate. The measurements were performed at rotation angles $\theta = 0°$ (**a**), $\theta = 45°$ (**b**), and $\theta = 90°$ (**c**). All comparisons yield p values of 50–95%, indicating an agreement, and thus clearing the candidates as genuine objects

learn about their presence. Given that this study focuses on a scenario where a bare pit undergoes verification, the list of the elements that would be of significant quantities is limited to the actinides and gallium, which is used to stabilize the plutonium in its δ-phase. Nevertheless, to address possible concerns, the treaty signatories can agree that the host will put samples of all elements that contain resonances in the agreed-upon range in their encrypting filters. In this manner, the inspectors will not be able to determine whether the absorption lines come from the weapon or the filter. The problem also has a technological solution. A neutron-opaque chopper synchronized with the neutron pulse can be added to the beamline, with an opening chosen such that it only lets through neutrons of a specific energy range. For example, for this experiment the [1, 50]-eV range translates to TOF of [150, 1061] μs. With an accelerator pulse rate of 25 Hz, a chopper rotating at 12.5 Hz would need two 41°-wide openings centered at 27.25° and 207.25° phases relative to the pulse to pass only the [1, 50]-eV neutrons. This opening angle and the rotation phase can be tuned to match the desired energy range, including that of a single resonance. Any hoaxing attempts involving shifting of phase or frequency would be readily exposed by the TOF data.

Finally, the chain of custody for the selection of the genuine object and its tamper-proof transportation to the dismantlement and verification facility is an important topic. Past literature has discussed various approaches for achieving this goal[6,28,29]. Exercises by the US and European national laboratories and organizations have taken place to test and characterize series of techniques necessary for this goal. The Letterpress Exercise in particular has focused on the high-level procedure, as well as the various simple but robust tamper-proof methods. Such techniques include electrical, mechanical, as well as reflective particle tag seals. Many of these low-tech methods use a physical randomness to ensure that a broken seal cannot be faked or reproduced. For a detailed discussion, see Smartt and Marleau[22] and Bunch et al.[28]. In addition to the particularities of the chain of custody, the arms control treaties stipulating verified dismantlement will have to negotiate the various conditions under which a particular verification technique is applied. For the method described in this study in particular, the two sides should negotiate the following parameters: the measurement time, beam current, and the resulting statistics, such that it is sufficient to detect the likely hoaxes without raising any worries about excessive information; the minimum count rate to be observed by the detector, derived from broad considerations of the weapon material quantities, as a way of ensuring that the hosts do not add neutron-opaque materials to the encrypting filter and thus make the measurements impossible; the manner in which the detector and source instrumentation will be validated before and after the measurements, as a way of ensuring that no hoaxing and no information leakage has occurred. Generally, the use of physical cryptography makes the acquired data fundamentally encrypted, thus significantly reducing information security risks associated with the instrumentation that acquires the data. However,

Table 1 Statistical comparisons between the candidates and the genuine reference object

Candidate object Mo/W composition and shape	rotation	χ^2/NDF	*p* value	Decision
Isotopic hoaxes				
50/50, cylinder	0°	5491/1198	0.00	Reject
10/90, cylinder	0°	10957/1175	0.00	Reject
Geometric hoax				
90/10, cube	0°	1196/1216	0.42	Accept
	45°	1532/1225	0.00	Reject
	90°	1823/1245	0.00	Reject
Honest candidate				
90/10, cylinder	0°	1140/1218	0.94	Accept
	45°	1124/1224	0.98	Accept
	90°	1234/1245	0.58	Accept

The composition here refers to the relative lengths along the *z* axis of molybdenum/tungsten components of the candidate objects. The total length of the objects is kept identical to that of the genuine reference. The genuine reference is a cylinder of the length of 3 cm and Mo/W composition of 90/10. In order to pass inspection, the objects have to first pass the χ^2 test along the *z* axis ($\theta = 0$) and then along two rotations at 45° and 90°. The procedure is shown to accept all honest candidates and rejects both isotopic and geometric hoaxes

validation of the instrumentation can further strengthen confidence. To this end, the inspection side could be asked to provide n copies of the instrumentation package, with the option for the hosts to perform invasive validation of the $n-2$ copies, leaving the last two copies to be used interchangeably in the verification exercises. In this case, the probability of the inspecting party to introduce two malicious packages undetected is $p = \binom{n}{2}^{-1} = 2/[n(n-1)]$. It should be clarified that we make no claims that the concept proposed in this study is a zero-knowledge proof. Physical cryptography implies a degree of information security less than zero knowledge, with a goal of protecting most useful information but not necessarily all information. The considerations listed in this section are only part of a larger set of possible circumstances to consider. As is the case with most cryptographic schemes, future research should focus on the pursuit of possible vulnerabilities and for solutions for those.

Discussion

Past arms control treaties lacked a method for reliably verifying the dismantlement of the nuclear weapons and instead focused on the delivery systems, such as ICBM and strategic bomber aircraft. This work experimentally demonstrates the feasibility of using resonance phenomena via epithermal neutrons transmission to compare two objects and verify that they are isotopically and geometrically identical, as part of a template verification exercise. Any differences in isotopics and geometry between the candidate and the genuine reference object can be detected via isotope-sensitive measurements by using multiple rotations. Similar to the requirements of zero-knowledge proof, the inspectors cannot learn significant information about the object itself and at most can infer the combined mass and isotopics of the object and the encrypting filter. These combined inferred quantities thus constitute upper bounds for the object, corresponding to the scenario of an empty encrypting filter. It is shown that by selecting thicker encrypting filters of just 1–2 kg of WGPu these upper bounds can be made large enough to make it impossible to infer any useful, new information. Unlike most information-barrier concepts, the sensitive information is encrypted in the physical domain, thus achieving a very high degree of information security. For an in-depth discussion, see the sections on information security in Hecla and Danagoulian[17]. Using the neutron beam at an experimental facility similar to the one described in this study, the measurements can be performed in the combined time of less than an hour.

Additional and continued research in security studies arena and by the weapons laboratories is needed to address the various high-level political and technical aspects of a treaty that would employ the techniques described in this study. In particular, the joint chain of custody is paramount to the validity of the genuine object, which establishes the template. While no treaties stipulating the verified dismantlement of the weapons have been enacted, exercises by US and European national laboratories and institutes have explored the various real-world considerations, testing a variety of protocols and techniques to insure a secure chain of custody[22]. This study presents only a basic concept, which will need to be embodied in particular designs adapted to the particular treaty conditions and the characteristics of the available facilities and instrumentation.

Finally, research needs to be performed to study the feasibility of this technique in more compact, possibly relocatable systems. The work presented in this study used a large facility due to its convenience and the high-precision neutron beam that it produced. However, smaller, more compact neutron sources may also enable such measurements. Such sources could be in the form of a pulsed deuterium–tritium generator or small, commercial, linear accelerator-driven sources that use bremsstrahlung beams to produce neutrons via (γ, n) reactions. The later systems are advantageous due to the large neutron flux that they would generate and would be similar to the facility used for this work, albeit at much smaller, laboratory-size scales. While this study focused on the verification of plutonium components of a disassembled weapon, the advent of higher-intensity neutron sources, e.g., using laser-driven methods[24,25], may allow for the verification of fully assembled weapons. The use of compact neutron source platforms may also allow for implementations of the technique described in this study using non-electronic detectors and preloads, similar to the concept by Philipe et al.[11], with the possibility of extending this physically cryptographic method to a fully zero-knowledge proof system.

Methods

Experimental facility. The experiment was performed at the 15 m station of the Gaerttner LINAC Research Center at the Rensselaer Polytechnic Institute. The neutron beam was produced via a 60 MeV electron beam from the LINAC, which produced 1-μs-long pulses with a repetition of 25 Hertz. An electronic signal from the pulse sets the start time t_0 necessary for the TOF calculation. The beam was incident upon a tantalum photoneutron target. Tantalum, due to its high atomic number, is a powerful source of bremsstrahlung photons when impinged by electrons. At 60 MeV, most of the energy loss by the electrons is radiative, i.e., via bremsstrahlung electromagnetic radiation. At the same time, the nucleus of ^{181}Ta has a photoneutron production threshold of 7.6 MeV, via the ^{181}Ta(γ, n)^{180}Ta reaction. The cross-section for this reaction peaks to approximately 0.37 barns at 14.7 MeV. Since the energy distribution of the bremsstrahlung photons is continuous, most of the photons overlap with the energy domain at which the photodisintegration of ^{181}Ta is at a maximum. The neutrons have an energy that is $E_n = E_\gamma - 7.6$ MeV, where E_γ is the energy of the bremsstrahlung photon. Thus most of the neutrons are produced in the $\mathcal{O}$(MeV) range. To produce an epithermal beam, a 2.54 cm polyethylene target was placed near the tantalum target, allowing a small fraction of the fast neutrons to undergo elastic scattering on the hydrogen in polyethylene and thus lose energy in a process referred to as moderation. The resulting neutron energy distribution spans 13 orders of magnitude from fast, MeV scale to the thermal, meV scale. For a detailed description of the facility and the target design, see Section I in Danon et al.[30].

The resulting polyenergetic neutron beam was then transported via a beamline to the 15 m station, named so because of the target to detector distance of approximately 15 m. A ^{6}Li glass detector detected the neutrons and registered their arrival times relative to the t_0 of the electron pulse. The neutron detector consisted of 3-mm-thick lithium glass scintillator with 6.6% lithium content, enriched to 95% in ^{6}Li. The scintillator is also sensitive to photons; however, the photon arrival

times would be $\mathcal{O}$(50ns) and thus could be rejected during the TOF analysis. Additional photons are present during the neutron arrival times, primarily due to (n, γ) capture of the thermalized neutrons near the detector volume. Those events, however, can be suppressed owing to the relatively weak light output by photon interactions in the scintillator. The only remaining background in the TOF analysis is the epithermal and thermal neutrons that scattered around the beamline. This effect can be seen, for example, as the counts at the bottom of the 15–30 eV absorption lines in Fig. 3. This background, however, is constant, does not change between multiple measurements, and thus does not affect the comparisons performed in this study. For a detailed description of the detector, the data acquisition electronics, and the general experimental set-up, see Section II in Danon et al.[31].

Energy reconstruction via TOF and statistical analysis. Owing to a thermalization times of $\lesssim$1 μs and flight times of ~ms, the pulse t_0 amounted to an good initial measure of the epithermal neutron emission time. The detection of the neutron in the scintillator produces a second pulse with a time t, and the energy of the neutron can be then inferred from $E = m(d/t_{\mathrm{tof}})^2/2$, where $t_{\mathrm{tof}} = t - t_0$. During the analysis of the data, however, it became apparent that the slight dependency of the moderation time on resulting neutron's energy significantly distorted the energy reconstruction. This effect was particularly significant for the higher-energy neutrons in the spectrum. To quantify this effect, simulations of this process were performed for the known geometries of the moderator, using the Geant4 object oriented simulation toolkit[32]. The energy-dependent corrections for thermalization time, which varied in the 4–8 μs range, were applied to the data, resulting in a precise reconstruction of the known molybdenum and tungsten resonances up to 200 eV.

The energy dependence of the detected neutrons in the open beam varied significantly with energy. This was caused in part by the intrinsic neutron flux, which changes significantly due to the incident neutron spectrum, caused by the underlying moderation process in the polyethylene moderator. It is also caused by the decreasing sensitivity of the ^{6}Li glass detector with increased energy, due to the power-law dependence of the ^{6}Li$(n, t)^4$He reaction, which has the form of $\sigma \propto E^{-1/2}$. The data acquisition of the facility bins the counts in 0.1-μs-wide time bins in the 1–200 eV range. When converting to the energy via TOF, the TOF distribution, which can be described as the time differential of the cumulative counting probability $\mathrm{d}P/\mathrm{d}t$, is weighted by the Jacobian, $\mathrm{d}E/\mathrm{d}t = -2E/t_{\mathrm{tof}}$, such that $\mathrm{d}P/\mathrm{d}E = \frac{\mathrm{d}P}{\mathrm{d}t}/\left|\frac{\mathrm{d}E}{\mathrm{d}t}\right|$. All statistical errors are propagated accordingly to the final energy spectrum. Finally, to even out the statistics throughout the broad 1–200 eV range, the uniform binning is changed to a non-uniform binning, where increasingly larger bins are assigned with increasing neutron energy.

The resulting spectral data from a pair of measurements were compared in a χ^2 statistical test. Assuming normally distributed errors, it is defined as $\chi^2 = \sum_1^N (c_{0,i} - c_{1,i})^2/(c_{0,i} + c_{1,i})$, where c_0 and c_1 are the count arrays for the spectra undergoing comparison, and N is the total number of bins. Given a value of χ^2 and N, the probability, also known as p value, can be determined from the χ^2 distribution. p Value describes the probability that two spectra's differences are due to statistical fluctuations alone. A low p value, e.g., $\ll$1%, is indicative of statistical effects due to cheating by the hosts.

Data availability

All the data supporting the findings of this study are available from the corresponding author upon reasonable request.

Received: 9 May 2019; Accepted: 6 September 2019;
Published online: 30 September 2019

References

1. Kristensen, H. M. & Norris, R. S. United States nuclear forces, 2018. *Bull. At. Sci.* **74**, 120–131 (2018).
2. Kristensen, H. M. & Korda, M. Russian nuclear forces, 2019. *Bull. At. Sci.* **75**, 73–84 (2019).
3. Hecker, S. S. *Doomed to Cooperate: How American and Russian Scientists Joined Forces to Avert Some of the Greatest Post-Cold War Nuclear Dangers* (Bathtub Row Press, 2016).
4. Mattis, J. *Nuclear Posture Review*. Technical Report (Office of the Secretary of Defense, 2018).
5. Kristensen, H. M. in *Nuclear Safeguards, Security, and Nonproliferation* 3–35 (Elsevier, 2019).
6. Fuller, J. Verification on the road to zero: issues for nuclear warhead dismantlement. *Arms Control Today* **40**, 19 (2010).
7. Drell, S., Callan, C., Cornwall, J., Dyson, F. & Eardley, D. *Verification of Dismantlement of Nuclear Warheads and Controls on Nuclear Materials*. Technical Report. (MItre Corp MClean Va Jason Program Office, 1993).
8. Marleau, P. et al. *Report on a Zero-Knowledge Protocol Tabletop Exercise*. Technical Report SAND2015-5075 (Sandia National Laboratories, Los Alamos National Laboratory, 2015).
9. Yan, J. & Glaser, A. Nuclear warhead verification: a review of attribute and template systems. *Sci. Glob. Security* **23**, 157–170 (2015).
10. Glaser, A., Barak, B. & Goldston, R. A zero-knowledge protocol for nuclear warhead verification. *Nature* **510**, 497–502 (2014).
11. Philippe, S., Goldston, R. J., Glaser, A. & dErrico, F. A physical zero-knowledge object-comparison system for nuclear warhead verification. *Nat. Commun.* **7**, 12890 (2016).
12. Kemp, R. S., Danagoulian, A., Macdonald, R. R. & Vavrek, J. R. Physical cryptographic verification of nuclear warheads. *Proc. Natl. Acad. Sci.* **113**, 8618–8623 (2016).
13. Marleau, P. & Brubaker, E. *An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System*. Technical Report (Sandia National Laboratories (SNL-CA), Livermore, CA, 2016).
14. Gilbert, A. J. et al. A single-pixel X-ray imager concept and its application to secure radiographic inspections. *Nucl. Instrum. Methods Phys. Res. Sect. A Accelerators Spectrometers, Detect. Associated Equip.* **861**, 90–97 (2017).
15. Seager, K. et al. Trusted radiation identification system. In *Proc. 42nd Annual INMM Meeting* (Institute of Nuclear Materials Management, 2001).
16. Vavrek, J. R., Henderson, B. S. & Danagoulian, A. Experimental demonstration of an isotope-sensitive warhead verification technique using nuclear resonance fluorescence. *Proc. Natl Acad. Sci. USA* **115**, 4363–4368 (2018).
17. Hecla, J. J. & Danagoulian, A. Nuclear disarmament verification via resonant phenomena. *Nat. Commun.* **9**, 1259 (2018).
18. Chichester, D. L. & Sterbentz, J. W. *Assessing the Feasibility of Using Neutron Resonance Transmission Analysis (NRTA) for Assaying Plutonium in Spent Fuel Assemblies*. Technical Report (Idaho National Laboratory (INL), 2012).
19. Losko, A. et al. Energy-resolved neutron imaging for interrogation of nuclear materials. In *Advances in Nuclear Nonproliferation Technology and Policy Conference* (American Nuclear Society, 2016).
20. Bourke, M. A. et al. *Non Destructive Examination of Un/U-Si Fuel Pellets using Neutrons (Preliminary Assessment)*. Technical Report (Los Alamos National Lab. (LANL), Los Alamos, NM, 2016).
21. Philippe, S., Glaser, A. & Goldston, R. J. Zero-knowledge differential isotopic comparison of special nuclear materials. In *Proc. 57th INMM Annual Meeting* (Institute of Nuclear Materials Management, 2016).
22. Smartt, H. & Marleau, P. *An Overview of Chain of Custody Options for LETTERPRESS*. Technical Report (Sandia National Lab. (SNL-NM), Albuquerque, NM, 2016).
23. Fetter, S., Cochran, T. B., Grodzins, L., Lynch, H. L. & Zucker, M. S. Gamma-ray measurements of a Soviet cruise-missile warhead. *Science* **248**, 828–834 (1990).
24. Roth, M. et al. Bright laser-driven neutron source based on the relativistic transparency of solids. *Phys. Rev. Lett.* **110**, 044802 (2013).
25. Fernández, J. C. et al. Laser-plasmas in the relativistic-transparency regime: science and applications. *Phys. Plasmas* **24**, 056702 (2017).
26. Allison, J. et al. Recent developments in geant4. *Nucl. Instrum. Methods Phys. Res. Sect. A Accelerators Spectrometers Detect. Associated Equip.* **835**, 186–225 (2016).
27. Mendoza, E., Cano-Ott, D., Koi, T. & Guerrero, C. New standard evaluated neutron cross section libraries for the GEANT4 code and first verification. *IEEE Trans. Nucl. Sci.* **61**, 2357–2364 (2014).
28. Bunch, K. J., Jones, M., Ramuhalli, P., Benz, J. & Schmidt Denlinger, L. Supporting technology for chain of custody of nuclear weapons and materials throughout the dismantlement and disposition processes. *Sci. Glob. Security* **22**, 111–134 (2014).
29. ElBahtimy, H. Disarmament: security context and verification challenges. VERTIC Newsletter July–September, Issue 126 (2009).
30. Danon, Y., Block, R. & Slovacek, R. Design and construction of a thermal neutron target for the RPI LINAC. *Nucl. Instrum. Methods Phys. Res. Sect. A Accelerators Spectrometers Detect. Associated Equip.* **352**, 596–604 (1995).
31. Danon, Y. et al. Neutron total cross-section measurements and resonance parameter analysis of holmium, thulium, and erbium from 0.001 to 20 eV. *Nucl. Sci. Eng.* **128**, 61–69 (1998).
32. Agostinelli, S. et al. GEANT4: a simulation toolkit. *Nucl. Instrum. Meth.* **A506**, 250–303 (2003).

Acknowledgements

This work is supported in part by the Consortium for Verification Technology under Department of Energy National Nuclear Security Administration Award DE-

NA0002534. The authors are grateful for the support and encouragement from their colleagues within the Consortium of Verification Technologies. The authors thank the staff at The Gaerttner LINAC Research Center and Yaron Danon in particular for assistance with the experiment, as well as valuable suggestions and advice. The authors are grateful to Igor Jovanovic for valuable comments on the manuscript. The authors also thank Ethan A. Klein for cataloging the nuclear data for (n, γ) and (n, n') reactions on molybdenum and tungsten. We express our gratitude to Jacopo Bongiorno for help with equilibrium heat transfer calculations and to the reviewers for their insightful comments.

Author contributions

A.D. conceived the project. Both authors performed the experiments and analyzed the data. A.D. wrote the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information is available for this paper at https://doi.org/10.1038/s41467-019-12386-0.

Correspondence and requests for materials should be addressed to A.D.

Peer review information *Nature Communications* thanks Bhaskar Sur and other anonymous reviewers for their contributions to the peer review of this work.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.