NUCLEAR DISARMAMENT VERIFICATION BASED ON (n,) REACTION USING PHYSICAL ENCRYPTION TECHNOLOGY

by

Qing-Hua HE [1,2*], ***Xiao-Suo HE*** [1], ***Tian LI*** [1], ***Kai-Kai LU*** [1], ***Sheng-Kai WANG*** [1], ***Xiao-Min DOU*** [1], *and* ***Xiao-Tao HE*** [1]

[1]Department of Nuclear Science and Technology,
Nanjing University of Aeronautics and Astronautics, Nanjing, China
[2] Key Laboratory of Nuclear Technology Application and Radiation Protection in Astronautics,
Nanjing University of Aeronautics and Astronautics, Ministry of Industry and Information Technology, Nanjing, China

Scientific paper
https://doi.org/10.2298/NTRP2202167H

To reduce the risk of leaking confidential information in nuclear arms control, we propose a new arms control inspection concept based on neutron activation analysis, in conjunction with physical shielding technology to distort the energy and propagation path of the outgoing particles in the physical domain. The reliability and security of this authentication concept are demonstrated using Monte Carlo simulations. It turns out that the concept can readily identify isotope cheats and two typical geometric cheats without revealing sensitive information about the inspected items.

Key words: nuclear disarmament verification, radiographic encryption, Monte Carlo simulation

INTRODUCTION

As being the central issue for national security concerns and international affairs [1, 2], future nuclear arms limitation agreements may expand the scope of restrictions such as the total number of nuclear weapons and warheads in the arsenals [3], to effectively and peacefully navigate the perils of the nuclear age in the future [4]. In subsequent rounds of arms control negotiations, new approaches to verifying nuclear warheads will be necessary. Verification of the authenticity of nuclear weapons, including undeployed warheads in nuclear arsenals and sometimes even of a single warhead, is necessary for contracting countries to fulfill their obligations faithfully.

A viable verification method should ensure a high degree of confidence in the authenticity of nuclear warheads while at the same time ensuring the confidentiality of sensitive information [3, 5]. In recent years, considerable research has been conducted on the issue of nuclear arms control in a new era. There are two main categories of these rapidly developing methods of verification: attribute-based and template-based. Using the attribute method, nuclear warheads and their components (*e.g.*, isotopic ratios, plutonium masses, *etc*.) can be determined. The template comparison method compares data from trusted reference items with the declared item.

To protect sensitive data, proposed inspection methods primarily employ information barrier technologies, such as low-resolution gamma radiation imaging [6], zero knowledge protocol [7, 8], and resonance fluorescence technique with encrypted foils [9]. Most methods proposed so far are still vulnerable to spoofing or leaking sensitive information [10]:
– the slightly *intrusive* verification technology can easily identify fraud scenarios, but it increases the risk of sensitive information being leaked,
– as a result of the complex electronic circuit system, the measurement data is more vulnerable to eavesdropping and tampering, and
– the limited information obtained through the *information barrier* detection leaves the verification party (inspectors) with insufficient confidence in the authenticity of the declared nuclear warheads, such as through some passive measurement techniques [11].

Recently, a verification method [12] combining physical methods and algorithms for double encryption has been developed, providing us with a new research direction.

Theoretically, proving a warhead's authenticity requires a verification system that satisfies necessary and sufficient conditions and meanwhile a mandatory political requirement: zero disclosure of sensitive information [9]. The necessary and sufficient conditions re-

* Corresponding author, e-mail: hegh@nuaa.edu.cn

quire that the system is sound and complete, meaning no false warheads can ever be proven true and all true warheads will be proven true. Following these requirements, Kemp *et al*. [9] proposed a special axiom to connect the physical measurements of warheads and statements about authenticity. The candidate warhead is authentic only if every manifold in a tested one is identical in size, shape, spatial relation, density, and isotopic composition to a corresponding manifold in an authentic warhead. Any valid verification system is a trade-off between this ideal axiom and the requirement of zero disclosure of sensitive information.

To meet these new requirements for nuclear arms control verification, cryptographic tools should be employed in the physical field, and methods similar to information-barrier with intrusive and complicated electronic circuitry should be avoided as much as possible.

To further improve the robustness of the verification system under zero leakage of confidential information, we propose a single-pixel-based nuclear warhead verification system using neutron-induced (n, γ) reaction to illuminate an object. This system runs under the necessary and sufficient conditions that all materials are in the appropriate location and no possibility of material substitutions to isotopic specificity. We also introduce a rotatable 2-D-randomly-attenuate photon shielding mask (rotatable mask) as a physical cryptographic tool to encrypt the confidential information of the inspected items in the physical domain not relying on electronics or software. In addition, a relevant verification protocol is correspondingly developed. Using numerical simulations, the reliability of this inspection system is verified, and the security and robustness of the system are also evaluated.

VERIFICATION SYSTEM

The verification system mainly contains a neutron activation analysis (NAA) component, a rotatable mask, and a single-pixel photon detector. The NAA component gains isotope-specific information about the inspected items, via exploiting neutrons of 0.025 eV in energy to activate the fissile components which decay primarily through emitting photons that provide a unique fingerprint of the inspected item.

A physical encryption technique using a photon shielding mask with non-uniform surface density is adopted in the physical domain to encrypt the energy and propagation path information carried by photons from the NAA process. The rotatable mask is placed between the inspected item and the photon detector, which rotates in a proposed sequence at the beginning of the measurement. The photons passing through the mask compose the encrypted *fingerprint* of the inspected item. By comparing this *fingerprint* data to that of a real item (template sample), the authenticity of the inspected items can be confirmed.

Since an ideal shielding mask with non-uniform surface density does not exist, in practice we produce it through coding a photon attenuation shielding plate and rotating it discretely in the verification. During installation, the screen can be embedded into the wall of the shielding room and makes a specific rotational motion when measuring, which could distort and encrypt the original signal. At the end of the verification system, a single pixel gamma detector [13] is placed to detect the transmitting photons.

VERIFICATION PROTOCOL

As a critical part of any nuclear warhead verification system, a valid verification protocol will guarantee that the inspectors gain high confidence in the authenticity of inspected items while no confidential information of them is exposed [14]. In our work, we propose the corresponding verification protocol.

Preparation work

Get reference warheads: a credible reference warhead is mandatory in the template comparison method, whereas how to get it should not be an easy task. Here are two suggestions for getting reference warheads. One is that the reference warhead could be chosen randomly from a deployed intercontinental ballistic missile (ICBM) during an unannounced visit by inspectors, which the selected warhead could be expected to be real [15]. Furthermore, if a reference warhead needs to be taken from undeployed nuclear warheads, a credible regulatory record is needed to confirm the authenticity of the warhead. Until all verification steps are completed, the selected reference warheads must be jointly supervised by both sides. And they can be monitored with strong regulatory measures [16], to prevent them from being replaced or tampered with.

Preparation of experimental equipment: hosts (the inspected party) shall prepare multiple rotatable masks separately, and the relevant construction information shall be kept secret from the inspectors. Meanwhile, hosts and inspectors need to prepare multiple gamma detectors jointly.

Select device

Before formal verification, detectors and rotatable masks for inspection are selected by inspectors to increase their participation. The coded pattern of the rotatable mask must be kept strictly confidential from the inspectors.

Experimental layout

Hosts extract the fissile components of the warheads and place them into visually opaque boxes to protect the geometry information of the warhead. At

the same time, the outer surface of the box is marked for alignment in the measurement. Two parties then work together to determine the irradiation orientation as well as the initial position of the tested item and the detector. Note that the irradiation direction of the inspected items should be consistent according to the marking.

Formal verification

In the measurement, the rotatable mask, which rotates discretely about its cylindrical axis is placed between the inspected item and the gamma detector, the rotation sequence or rotation step of which could be determined by both parties. The inspected item will now be directly exposed to the neutron source, and both parties will be able to monitor the flux of the source using their respective equipment. As a result of the (n, γ) reactions, the prompt gamma rays are randomly attenuated by the screen and detected by the single-pixel gamma detector. The same process is repeated for the reference item to obtain a reference fingerprint for comparison.

Template comparison

The authenticity of the inspected item is determined based on the template comparison method in which an encrypted gamma signal is compared to that from a trusted template item. Mathematically, a criterion is set to determine the authenticity of the inspected item, the detail of which will be given in the following sections. If it is confirmed that the submitted item is not fraudulent, the nuclear materials contained in them can be destroyed [17].

In this protocol, only the pattern of the rotatable mask is kept secret from the inspectors and other processes can be completed jointly by both parties, which greatly increases the participation of the inspectors and improves the credibility of the verification results.

NUMERICAL SIMULATION

To show how the verification system is implemented, we use numerical simulations to demonstrate the validity of this method. A simplified verification system, based on the Geant4 toolkit (version: geant4.10.04. p02) [18], is constructed as shown in fig. 1, and three fraud scenarios are used to test the feasibility of the system.

A thermal neutron source with an energy of 0.025 eV is used to irradiate the inspected items, which could stimulate the excited gamma signal that comes from the fission components of nuclear weapons via (n, γ) reactions. To encrypt the sensitive information of the outgoing gamma rays in the physical domain, in the simulation we constructed a lead plate composed

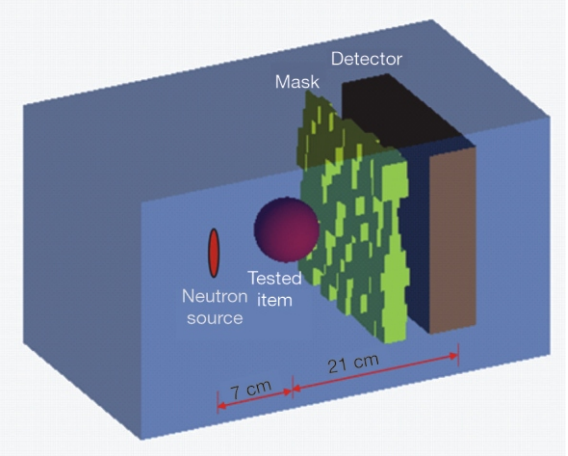

Figure 1. Schematic diagram of the verification system

of a 10 10 set of lead modules in the shape of a regular quadrangular prism, the lengths of which vary randomly from 0 cm to 6 cm at every time the photon counting information is collected. This random shielding lead mask will randomly attenuate photon energies and distort their propagation path so that the final photon counts in the counter area vary with the mask of different structures. Therefore, instead of the rotatable mask, we used a random mask with an ever-changing structure in the simulation. Behind the random mask, a single-pixel detector was simulated to detect gamma signals that have been encrypted through the random mask.

In combination with the template comparison method, we only need to ensure the same experimental conditions between the control groups. Directly simulating the detector is therefore unnecessary, and we simply set a rectangular gamma detection area with a detection threshold of 100 keV (to reject background signals) at the end of the verification system.

A total of 40 samples were set up in this simulation, including 1 reference sample, 10 real samples, and 29 cheating samples. The real samples are identical to the reference sample, whereas the cheating samples differ from the reference sample in terms of isotopic ratios and geometric structure, which includes two cheating scenarios involving removal and size changes. The shapes of all samples in this study are typically set as hollow spherical shells to simulate the fissile component of the nuclear weapon. The specific parameters of reference samples, real samples, and cheating samples of different isotope ratios are listed in tab. 1. The cheating samples of removal are that the inner diameter of the spherical shell increases gradually, while isotope ratio and outer diameter remain consistent with the reference sample, to simulate the deceptions by hosts who cut corners to preserve part of the nuclear material. Similarly, the cheating samples of size change reduce their outer diameter gradually while the volume and isotope ratio remain consistent with the reference sample that corresponds to the sce-

Table 1. Parameters of reference samples, real samples, and cheating samples in isotope ratio

	Isotope ratio	Inside radius [cm]	External radius [cm]
Reference sample	96 % ^{235}U, 4 % ^{238}U	3.00	5.00
Real sample	96 % ^{235}U, 4 % ^{238}U	3.00	5.00
Cheating sample in isotope ratio	56 % ^{235}U, 44 % ^{238}U	3.00	5.00

nario in which the hosts cheated with nuclear material that is less difficult to make industrially in the inspection. More details about the parameters of the above samples are shown in tabs. 2 and 3. The deception scenarios in which nuclear warheads are modified at the microstructural level are not considered, such as the grain size of metals, surface polish, and chemical isomers of similar densities [9]. We deem these hoaxes insignificant in this study since they do not simplify or reduce the cost of manufacturing.

Table 2. Parameters of cheating samples of removal

	Isotope ratio	Inside radius [cm]	External radius [cm]
Removel-1	96 % ^{235}U, 4 % ^{238}U	3.10	5.00
Removel-2	96 % ^{235}U, 4 % ^{238}U	3.20	5.00
…	…	…	…
Removel-9	96 % ^{235}U, 4 % ^{238}U	3.90	5.00
Removel-10	96 % ^{235}U, 4 % ^{238}U	4.00	5.00
Removel-11	96 % ^{235}U, 4 % ^{238}U	3.01	5.00
Removel-12	96 % ^{235}U, 4 % ^{238}U	3.03	5.00
Removel-13	96 % ^{235}U, 4 % ^{238}U	3.05	5.00
Removel-14	96 % ^{235}U, 4 % ^{238}U	3.07	5.00
Removel-15	96 % ^{235}U, 4 % ^{238}U	3.09	5.00
Removel-16	96 % ^{235}U, 4 % ^{238}U	3.001	5.00
Removel-17	96 % ^{235}U, 4 % ^{238}U	3.002	5.00

Table 3. Parameters of cheating samples of size change

	Isotope ratio	Inside radius [cm]	External radius [cm]
Size change-1	96 % ^{235}U, 4 % ^{238}U	0.849	4.62
Size change-2	96 % ^{235}U, 4 % ^{238}U	1.799	4.70
Size change-3	96 % ^{235}U, 4 % ^{238}U	2.326	4.80
Size change-4	96 % ^{235}U, 4 % ^{238}U	2.698	4.90
Size change-5	96 % ^{235}U, 4 % ^{238}U	2.731	4.91
Size change-6	96 % ^{235}U, 4 % ^{238}U	2.795	4.93
Size change-7	96 % ^{235}U, 4 % ^{238}U	2.856	4.95
Size change-8	96 % ^{235}U, 4 % ^{238}U	2.915	4.97
Size change-9	96 % ^{235}U, 4 % ^{238}U	2.972	4.99
Size change-10	96 % ^{235}U, 4 % ^{238}U	2.994	4.998
Size change-11	96 % ^{235}U, 4 % ^{238}U	2.997	4.999

RELIABILITY ANALYSIS

We validated the verification system by comparing the radiation measurements of simulated samples listed in the above tables with the result from the reference sample. The rotatable mask is rotated by a predetermined sequence at the beginning of the irradiation, and the measurement will stop after a period agreed upon by both parties. With each sample, we can obtain a unique *fingerprint*: K, the total number of photons detected as a function of the position of the rotatable mask rotating discretely. In addition, the reference sample (the template) has a fingerprint: K_{ref} with the same radiation measurements. By comparing the fingerprint of the sample to be tested with that of the template, we can determine whether the measured sample is consistent with the template.

In the template comparison method, a metric value D is used to quantitatively analyze the similarity of fingerprints between the measured samples and the template

$$D \quad \mu \quad \frac{(y_2 \quad y_1)^2}{y_1} \tag{1}$$

where, y_1 and y_2 are fingerprint sequences from the reference sample and the sample to be tested, respectively, where each fingerprint sequence consists of 100 sets of photon measurement. The closer the metric value D is to zero, the higher the similarity between the sample to be tested and the reference sample is. The receiver operating characteristic curve (ROC curve, a co-ordinate schema analysis tool used to set the optimal threshold in the same model) is used to assess the robustness of this verification system after measuring the 40 samples one by one.

For each sample, 100 irradiation measurements are made at a total source flux of 5 10^6 and an example of a typical fingerprint from a template is shown in fig. 2 along with some samples to be tested. Each fingerprint is made up of 100 total numbers of photon measurements, and each count is the result of the measurement of encrypted irradiation. The fingerprints were generated from the same rotation sequence, which could be determined jointly by both parties. By comparing the fingerprints of samples to be tested with that of the template, one can determine whether the inspected samples are true or not.

The ROC curve of the verification system without noise is shown in fig. 3, with false positive rate (FPR) as abscissa and ture positive rate (TPR) as ordinate. On the other hand, the area value under the ROC curve (AUC), an evaluation index of the model's merits, is used to investigate the accuracy of the verification system, and, a value as high as 0.93 indicates the system's accuracy is accepted.

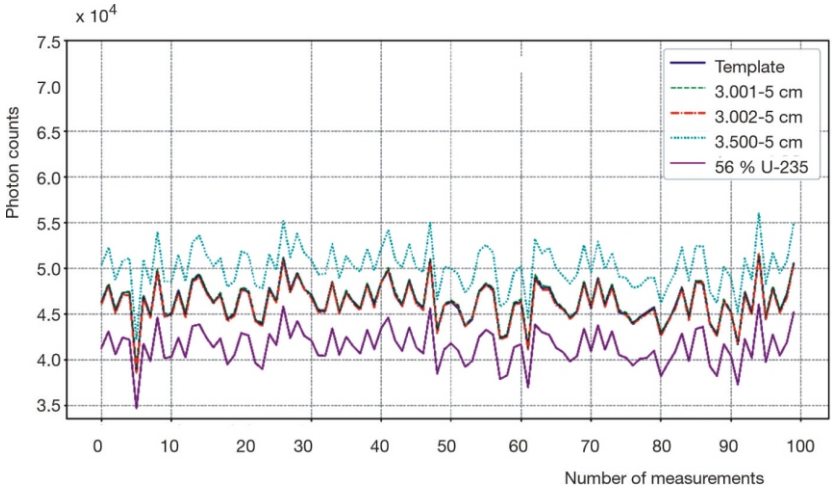

Figure 2. Typically measured fingerprints (time-series photon counts data from single photon detector) for different tested items

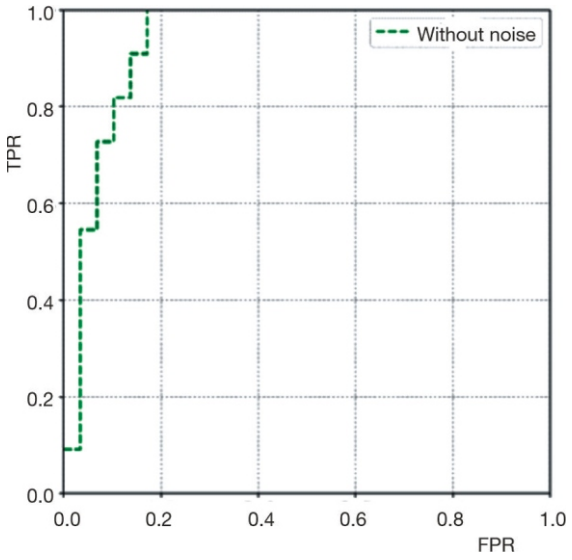

Figure 3. The ROC curve without the noise

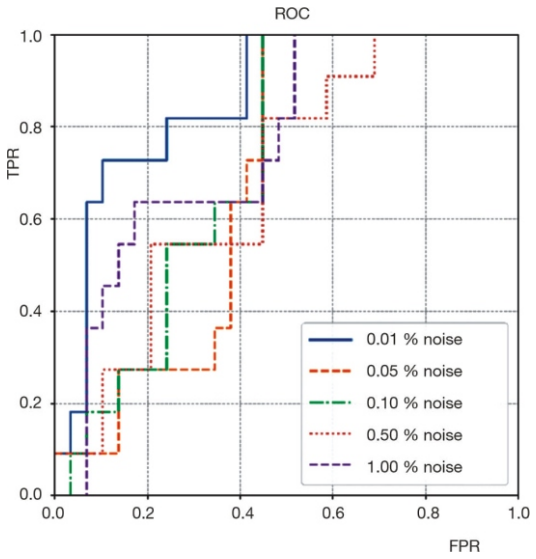

Figure 4. The ROC curve under different noise levels

STABILITY OF THE SYSTEM UNDER DIFFERENT NOISE LEVELS

To analyze the stability of the inspection method at different levels of noise, we add gaussian noise to the total number of outgoing particles during the simulation. According to the definition of SNR (the ratio): SNR = = (signalPower)/(noisePower), where signalPower and noisePower are the intensity of signal and noise respectively that could be calculated according to the following formula: signalPower = ($_{i\ 1}^{n}$ signal$_i^2$) / n, where n is the length of the signal. The σ_{noise} value could be determined by the equation: $\sigma_{\text{noise}} = \sqrt{(\text{signalPower} / \text{SNR})}$ when given a certain value of SNR. Thus, the Gaussian broadening of the total number signal N_i can be randomly sampled according to the following formula

$$G(N_i, \sigma_{\text{noise}}) \quad \frac{1}{\sigma_{\text{noise}}\sqrt{2}} \exp \quad \frac{(x \quad N_i)^2}{2\sigma_{\text{noise}}^2} \qquad (2)$$

The robustness of the system under different SNR is analyzed with a Monte Carlo simulation in which the neutron source flux is set to be 5 10^6. As shown in fig. 4, the ROC curves are used to measure the robustness of the system. The corresponding AUC values can be obtained by adding 0.01 %, 0.05 %, 0.1 %, 0.5 %, and 1 % noise, respectively.

It can be seen from fig. 5 that the AUC value is above 0.7 when 1 % noise is added, indicating that the system maintains excellent stability under different SNR and has high accuracy for judgment.

SAFETY ANALYSIS

Security is the primary consideration in any verification system. If the security of the sensitive information of the samples to be tested cannot be guaranteed, the hosts may terminate the verification at any time.

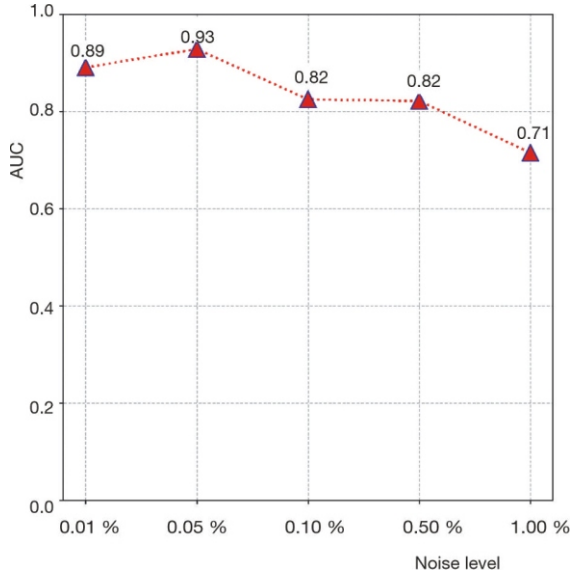

Figure 5. Values of AUC at different noise levels

In this verification system, we believe there are two main types of sensitive information about nuclear weapons:

– Geometrical structure information, such as mass, shape, arrangement, and distribution of nuclear materials;

– Isotope types and contents of nuclear materials. Based on the aforementioned robustness analysis of the verification system, we recorded the total number of gamma particles using a single-pixel detector. Therefore, the 2-D information of the tested items, such as shape and arrangement distribution, cannot be deduced from1-D counting data, which turns out to be computationally inadmissible [13]. According to the NAA formula

$$n \quad \frac{W}{M} N_A \eta \varepsilon_t \sigma_c \Phi f_\tau \tag{3}$$

where n is the intensity of the analysis peak, W – the content of the element to be measured, M – the atomic mass, N_A – the Avogadro constant, η – the isotope abundance, ε_t – the total detection efficiency, σ_c – the capture cross-section, Φ – the neutron flux rate received by the sample, and f – the gamma-ray branch ratio, the sensitive gamma spectrum cannot be measured from the single pixel time-series photon counts data, and so no one will be aware of the isotope information of the tested items.

The structure of the rotatable mask is kept secret from the inspector while its rotation sequence can be determined by both parties, which is equivalent to a different mask structure for each measurement. We construct a series of fingerprints encrypted by rotatable masks with different structures and quantify the probability of brute force cracking template fingerprints to measure the security of the rotatable mask. Set a coincidence rate P, that is, the probability of obtaining the same fingerprints under the masks of different structures. When the similarity of two fingerprints reaches a certain threshold, we consider it successful. In the authentication of security, we take the reference sample as an experimental object to generate one million fingerprints under `masks of different structures, and each fingerprint contains 100 measurements. One of the million fingerprints is randomly selected as the template, and the other fingerprints are compared with it in turn, so that nearly a million D values could be obtained according to the eq. (1).

As can be seen in fig. 6, the statistical result of D values can be approximately fitted as a Gaussian distribution with a mean value of 348.77 and a standard deviation of 42.02.

To calculate the probability of generating the approximate fingerprint of the tested items with the rotatable masks with different structures, we define a threshold value T. According to eq. (1), if the metric value D is less than the threshold value T when the fingerprint under test is compared with the reference fingerprint, we consider a successful brute-force cracking. To get a trusted T value, we perform a hundred irradiation measurements on the reference sample with the same rotatable mask and the same rotating sequence, then, one fingerprint was randomly selected as the reference object and compared with others, of which the 99 metrics D are shown in fig. 7.

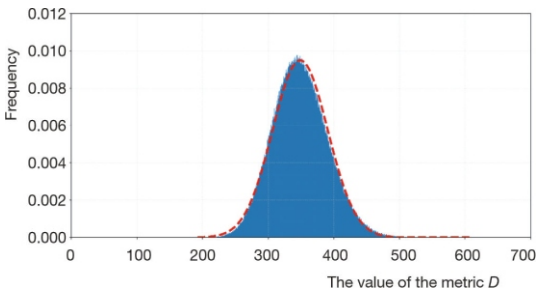

Figure 6. Frequency distribution of *D* values in security test of one million measurements

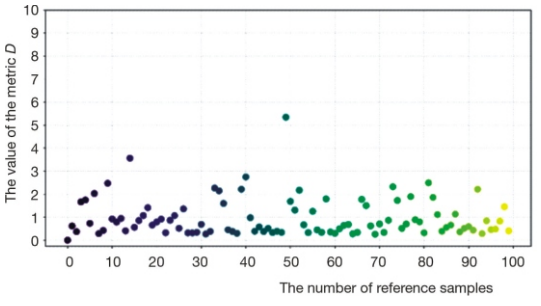

Figure 7. The value of the metric *D* of the fingerprints of 100 reference samples under the same measurement conditions

According to the above experimental results, the mean metric D of fingerprint similarity degree of the same sample under the same experimental conditions is about 0.93. If we take the T value as 1 here, the coincidence rate P is given to be

$$P \int_0^T \frac{1}{\sqrt{2\pi\sigma}} e^{\frac{(x-\mu)^2}{2\sigma^2}} dx \Big/ \int_0^1 \frac{1}{\sqrt{2\pi}\ 42.02} e^{\frac{(x-348.77)^2}{2\,42.02^2}} dx \quad 1.15\ 10^{-17} \tag{4}$$

According to the extremely low value of P it is hard to brute-force fingerprints on the tested items without obtaining the structure of a rotatable mask, so deriving the mass of nuclear material from an encrypted fingerprint will only be more difficult. Therefore, we believe that the rotatable mask can highly protect the sensitive information of the tested items.

Such a system based on the single pixel method prevents the inspector from detecting sensitive 2-D transport information, but it may be vulnerable to deliberate deception in which the host can adjust subtly nuclear material content and the thickness of the shell using self-shielding effects. This can be compensated by combing this method with neutron transport measurement which can effectively detect various geometric deceptions. In addition, adding different measurement alignments can also improve the security of this system. A better verification system needs a balance between security and robustness. Great efforts should be undertaken to test and improve the security and robustness of the proposed method in practical situations, where systematic uncertainties, small misalignments, or other environmental condition variations may bring new challenges that are hard to be predicted with numerical simulations.

In practice, developing a real nuclear warhead verification system will be a big challenge [14]. Although UK-Norway Initiative [19] opens the possibility of developing such a system by multiple countries (with or without nuclear weapons), there are still many obstacles to overcome in the practical undertaking.

SUMMARY

In this work, a new nuclear warhead verification system and protocol based on NAA is proposed, in conjunction with physical shielding technology to encrypt the energy and propagation path information of the outgoing particles in the physical domain. To demonstrate the feasibility of the system, three typical forgery cases are simulated, and the stability of the system under different noise levels is certified. It is verified to detect cheating scenarios of different isotope ratios, removal, and size change readily without revealing sensitive information about the inspected items. In the present work, the approach proposed can also be applied to the verification of encrypted personal data in situations such as biometrics, classified equipment identification, or other tasks involving customized radiation-based verification.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China, grant Nos. 11805099 and U2032138, and the Fundamental Research Funds for the Central Universities, grant Nos. NS2018043, NJ2020017-5, and the Foundation of Jiangsu Province high-level innovation and entrepreneurship talent introduction plan, grant No. 1006-KFR20052.

AUTHORS' CONTRIBUTIONS

The idea for this study was initiated by Q. H. He and X. S. He. Numerical simulation was performed by X. S. He. The manuscript was compiled by X. S. He, Q. H. He, and X. T. He. The literature search was performed by T. Li, K. K. Lu, S. K. Wang, and X. M. Dou. All the authors participated in the discussion of the presented results.

REFERENCES

[1] Kristensen, H. M,, Korda, M, United States Nuclear Forces, *Bulletin of the Atomic Scientists, 76* (2020), 1, pp. 46-60
[2] Kristensen, H. M., Korda, M., Russian Nuclear Forces, *Bulletin of the Atomic Scientists, 76* (2020), 2, pp. 102-117
[3] Yan, J., Glaser, A., Nuclear Warhead Verification: A Review of Attribute and Template Systems, *Science & Global Security, 23* (2015), 3, pp. 157-170
[4] Arbatov, A., Saving Nuclear Arms Control, *Bulletin of the Atomic Scientists, 72* (2016), 3, pp. 165-170
[5] Hinderstein, C., Cultivating Confidence: Verification, Monitoring, and Enforcement for a World Free of Nuclear Weapons, Hoover Press, 2013, USA
[6] Gottsche, M., *et al*., Low-Resolution Gamma-Ray Spectrometry for an Information Barrier Based on a Multi-Criteria Template-Matching Approach, *Nuclear Instruments & Methods in Physics Research Section A, 840* (2016), Dec., pp. 139-144
[7] Glaser. A., *et al*., A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol, *Proc. 53rd Annu. Inst. Nucl. Mater. Manag. Meet., Orlando, USA,* (2012), pp. 2395-2404
[8] Philippe, S., *et al*., A Physical Zero-Knowledge Object-Comparison System for Nuclear Warhead Verification, *Nature Communications, 7* (2016), 1, doi: 10.1038/ncomms12890
[9] Kemp, R. S., *et al*., Physical Cryptographic Verification of Nuclear Warheads, Proceeding, *National Academy of Sciences of the United States of America, 113* (2016), 31, pp. 8618-8623
[10] Li, T., *et al*., Research on Encryption Algorithm of Radiation Imaging for Nuclear Arms Control Verification, *Nuclear Electronics & Detection Technology, 40* (2020), 6, pp. 937-942
[11] Ziock, K. P., *et al*., A Gamma-Ray Imager for Arms Control, *IEEE Transactions on Nuclear Science, 39* (1992), 4, pp. 1046-1050
[12] He, Q. H., *et al*., A Physically Cryptographic Hoteling Observer for Nuclear Warhead Verification, *Nucl Technol Radiat, 36* (2021), 4, pp. 358-363
[13] Gilbert, A. J., *et al*., A Single-Pixel X-Ray Imager Concept and Its Application to Secure Radiographic

Inspections, *Nuclear Instruments and Methods in Physics Research, Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 861* (2017), July, pp. 90-97
[14] Glaser, A., *et al*., A Zero-Knowledge Protocol for Nuclear Warhead Verification, *Nature, 510* (2014), 7506, pp. 497-502
[15] Hecla, J. J., Danagoulian, A., Nuclear Disarmament Verification Via Resonant Phenomena, *Nature Communications, 9* (2018), 1, p. 1259
[16] Gerdes, E. R., *et al*., A Proposed Approach for Monitoring Nuclear Warhead Dismantlement, *Science & Global Security, 9* (2001), 2, pp. 113-141
[17] Drell, S., *et al*., Verification of Dismantlement of Nuclear Warheads and Controls on Nuclear Materials, Technical Report JSR-92-331 (Jason, Mitre Corp, Mclean, 1993), USA
[18] Agostinelli, S., *et al*., Geant4: A Simulation Toolkit, *Nuclear Instrumentation and Methods in Physics Research A, 506* (2003), 3, pp. 250-303
[19] Allen, K., *et al*., UK-Norway Initiative (UKNI) Approach for the Development of a Gamma Ray Attribute Measurement System with an Integrated Information Barrier [C], *Proceedings,* 35th ESARDA Symposium. Edited by F. Sevini. Bruges, Belgium. 2013

Received on June 9, 2022
Accepted on August 16, 2022

Ђинг-Хуа ХЕ, Сјао-Суо ХЕ, Тјен ЛИ, Кај-Кај ЛУ, Шенг-Кај ВАНГ, Сјао-Мин ДОУ, Сјао-Тао ХЕ

ВЕРИФИКОВАЊЕ НУКЛЕАРНОГ РАЗОРУЖАЊА ЗАСНОВАНО НА (n,) РЕАКЦИЈИ КОРИШЋЕЊЕМ ТЕХНОЛОГИЈЕ ФИЗИЧКОГ ШИФРОВАЊА

Да бисмо смањили ризик од цурења поверљивих информација при контроли нуклеарног наоружања, предлажемо нови концепт инспекције контроле наоружања заснован на анализи неутронске активације у спрези са технологијом физичке заштите – да би се изменила енергија и путања ширења одлазних честица у физичком простору. Поузданост и сигурност овог концепта оверавања демонстрирани су коришћењем Монте Карло симулација. Испоставило се да концепт може лако да идентификује изотопске преваре и две типичне геометријске варке без откривања осетљивих информација о прегледаним предметима.

Кључне речи: верификовање нуклеарног разоружања, радиографско шифровање, Монте Карло симулација