Physical Cryptographic Warhead Verification

Areg Danagoulian

MIT
VERIFICATION

• How do treaty partners verify that the other side is dismantling actual warheads and not fakes? They don’t.

• Verification: delivery vehicles – easier to verify.

• Problems: large leftover of non-deployed warheads
  • theft → nuclear terrorism, nuclear proliferation

→ Authenticate warheads, without revealing secret information
Previous Research: information barriers, *attribute* verification

- Developed at US national labs and AWE (UK)
- Electronic Information Barrier – perform measurements, light up red/green lights. No direct access to classified data.
- Verify the *attributes* of a weapon:
  - is there plutonium inside? ✔
  - High-Explosives present? ✔
  - etc. ✔

- → risk of diversions/spoofing

- The *info. barriers* are in electronics/software → backdoors, hacks, software exploits → risk of information leakage
Our Research: physics-based cryptography, template verification

Authenticated template “golden copy” of W88
Picked from a randomly selected ICBM

Candidate copies, W88

Is $A_0 = A_1$? ✓
$A_0 = A_2$? ✓
$A_0 = A_3$? ✓

Challenge: perform checks while
• protecting secrets without relying on electronic/soft. barriers
• no fakes
• type II error $<< 1$

→ need a physical cryptography – use NRF!

To dismantlement
Analogy: NRF to Optical Spectroscopy

Optical Spectroscopy

- Continuous Spectrum
- Emission Spectrum
- Absorption Spectrum

Nuclear Spectroscopy

- Bremsstrahlung
- Back-scattered NRF
- Transmitted NRF

Absorption lines, ~eV

(W. Bertozzi)

NRF: unique fingerprint of isotopics
Nuclear resonance fluorescence (NRF) is used to make isotope-specific measurements. Absorption and emission energy determined by nuclear energy levels.
Broad-spectrum photon sources access more nuclear levels

different line spectra for U-235, U-238, Pu-239, Pu-240...
NRF Weapon authentication Concept

Hosts:
- provide the candidate warheads (to be authenticated)
- Foil – thickness unknown to the inspectors, but of agreed upon isotopes

Inspectors:
- Detector, electronics (to be verified by hosts)
- Visual access to the foil

Joint:
- Template (“golden copy”)
NRF Weapon authentication Concept

Weapon B: candidate

- **Physical Cryptography:**
  - No direct data from the weapon itself
  - \( \text{SIGNAL} = (\text{Weapon}) \otimes (\text{Foil}) \)
  - Impossible to extract (Weapon)

- **Soundness and completeness:**
  - Authenticated template A -- acquire \( S_{\text{NRF}}(A) \)
  - Candidate weapon B -- acquire \( S_{\text{NRF}}(B) \)
  - and compare

Bremsstrahlung (X-ray)
NRF filtered brem

Shielding

Foil

Everything classified by the host

Everything open

1.6 1.8 2.0 2.2 2.4 2.6 2.8 3.0 3.2 3.4

1.6 1.8 2.0 2.2 2.4 2.6 2.8 3.0 3.2 3.4

A

B
NRF Weapon authentication Concept

Weapon A: authenticated template

Foil

Everything classified by the host

Bremsstrahlung (X-ray)

NRF filtered brem

Weapon B: candidate

Foil

Everything open

Shielding

Signal = (Weapon) ⊗ (Foil)

\[ \Phi_{nrf}(E) \propto \phi_{brem}(E) \exp(-D(\mu_{nrf} + \mu_{nr})) \left[ 1 - \exp\left(-X\left(\mu_{nrf} + \mu_{nr} \frac{1 + \cos \theta}{\cos \theta}\right)\right) \right] \]
Simulated 2.1 or 2.5 MeV bremsstrahlung beam

> 1000 core hours for sufficient NRF statistics
WGPu → U-238 replacement hoax

Genuine template

U-238 hoax
Canonical hoax scenarios are detectable in tens of minutes

<table>
<thead>
<tr>
<th>Hoax scenario</th>
<th>Strongest discrepancy (σ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WGPu $\rightarrow$ U-238</td>
<td>107</td>
</tr>
<tr>
<td>WGPu $\rightarrow$ FGPu</td>
<td>14.6</td>
</tr>
<tr>
<td>Geometric hoax, 0°</td>
<td>1.16</td>
</tr>
<tr>
<td>Geometric hoax, 10°</td>
<td>6.38</td>
</tr>
<tr>
<td>Geometric hoax, 30°</td>
<td>49.7</td>
</tr>
</tbody>
</table>

NRF experimental setup

- 2.5MeV e\(^-\) beam
- 3mm DU
- 2.5” Al (for normalization)
- Data:
  - NRF (HPGe)
  - Current readout (radiator)
  - Brem (\(\gamma\) detector)
- Use data to validate the MC model
- Basic tests before the POC
The three major U-238 resonances (and branches) are clearly observed.
Nuclear Resonances \(\rightarrow\) Isotopic fingerprinting

NRF by no means the only resonance! Others? Epithermal Neutrons!

May have stronger *information security*; more *compact*; *faster*; equivalent hoax *sensitivity*. **Paper in review.**

For more – come to American Nuclear Society (ANS) on 10/23!
Future

• Moving from simulations to experimental proof-of-concept
  – Validated semi-analytical model for NRF count rates in physical cryptography experiments
  – Information security.
  – Upcoming transmission experiments!
  – Epithermal neutrons? Stay tuned!
Physical cryptography collaboration

Faculty:

Prof. Areg Danagoulian
Prof. Scott Kemp
Dr. Richard Lanza

Stanton post-doctoral fellow:

Brian Henderson

Graduate students:

Jayson Vavrek
Ruaridh Macdonald
S Jeremiah Collins
Jake Hecla
Current Inventory

2017 Estimated Global Nuclear Warhead Inventories

The world’s nuclear-armed states possess a combined total of roughly 15,000 nuclear warheads; more than 90 percent belong to Russia and the United States. Approximately 9,600 warheads are in military service, with the rest awaiting dismantlement.

Geometries and Tomography

- tNRF based system – single pixel camera.
- A single measurement can hide “ghosts” \(\rightarrow\) good material sensitivity, but no sensitivity to geometric hoaxes
- Take measurements/projections under different random angles
- Making a fake weapon which matches is possible, but…
- A ghost can be broken down into a Zernike Polynomial with order > possible projections \(\rightarrow\) better angular resolution means a more complex hoax.
- Chance of undetected cheating:

\[
P = \prod_{i=0}^{k-1} \frac{M-i}{N-i}
\]

for \(k = 2, N \sim 60, M \sim 5, P = 0.5\%\)

\(\rightarrow\) geometric hoaxes are possible, but too complex to be valuable

R.S. Kemp, R. Macdonald
What is physical cryptography?

- SIGNAL $\rightarrow$ PHYSICAL PROCESS $\rightarrow$ HASH
  - the HASH is unique to the original SIGNAL
    - $\rightarrow$ if two hashes match, then the underlying signals are also identical
  - the SIGNAL cannot be recovered from the HASH without additional key
- Binary information – yes/no
- Physical cryptography requirements similar to Zero Knowledge proof (Mikali-Goldwasser, 1989)
  - Soundness: a cheating prover will be caught (Type I error)
  - Completeness: a honest prover will be cleared (Type II error)
  - Zero knowledge: if the prover is honest, the verifier will learn nothing additional

- Problem at hand: prove that weapon A and B are identical, without revealing any additional information about the weapon
  - prover – host
  - verifier – inspection party

- Challenge: find the “PHYSICAL PROCESS”
  - Neutron transmission radiography
  - $\rightarrow$ transmission NRF!
Example: WGP $\rightarrow$ DU replacement hoax

$\Rightarrow$ hoax vs. template: discrepancies in every line except $^{235}$U