Thrust Area 5: Disarmament Verification Overview

Richard Lanza

MIT

National Nuclear Security Administration

Thrust Area 5: Disarmament Verification

Zero Knowledge NRF	S. Kemp, MIT
ZK Neutron Radiography	F. D'Errico, Yale
Information Barriers for Enhanced Automated Isotope Identification	C. Sullivan, UI

Zero Knowledge Using NRF

Scott Kemp
MIT

National Nuclear Security Administration

Motivation for Warhead Verification

Project CloudGap (1968): Even rudimentary measurements leak classified information

Temporary Solution: No warhead verification

Re-armament stability under crisis & loose nukes addressed only by verified warhead elimination

How to do it?

Provenance + unclassified measurements?

Electronic Information Barriers + templates?

Disc o' Doom!

Electronic Information Barriers + attributes?

Low selectivity. Currently favored approach.

And now for something completely different...

Zero Knowledge proofs (Goldwasser) can be used to prove warhead authenticity (Glaser).

A ZK proof demonstrates something is true without revealing why.

Any proof requires soundness & completeness. We further impose a zero-knowledge condition.

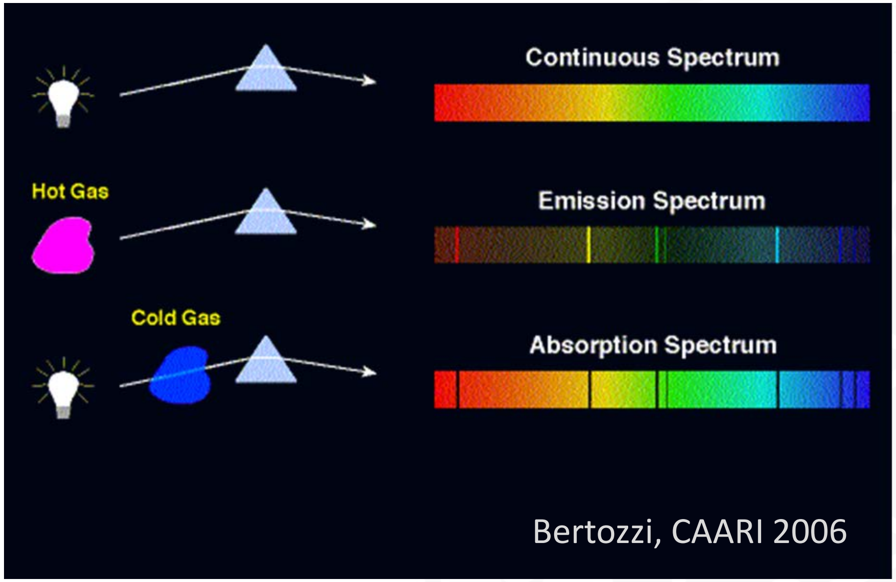
The MIT Team

• Areg Danagoulian	NSE
• John Fisher	EECS/CSAIL
• Shafi Goldwasser	EECS/CSAIL
• Zach Hartwig	NSE
• Scott Kemp	NSE
• Richard Lanza	NSE

- 1 PhD, 2 MS, and 2 UG students

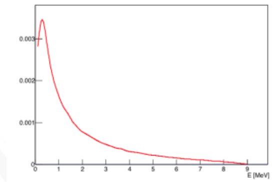
Analogy: NRF to Optical Spectrometry

Optical Spectroscopy

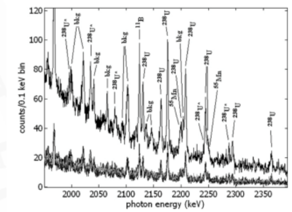


NRF Spectroscopy

Bremsstrahlung

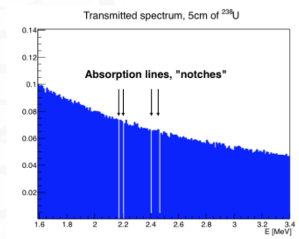


Back-scattered NRF



B. Quiter *et al.*

Transmitted NRF

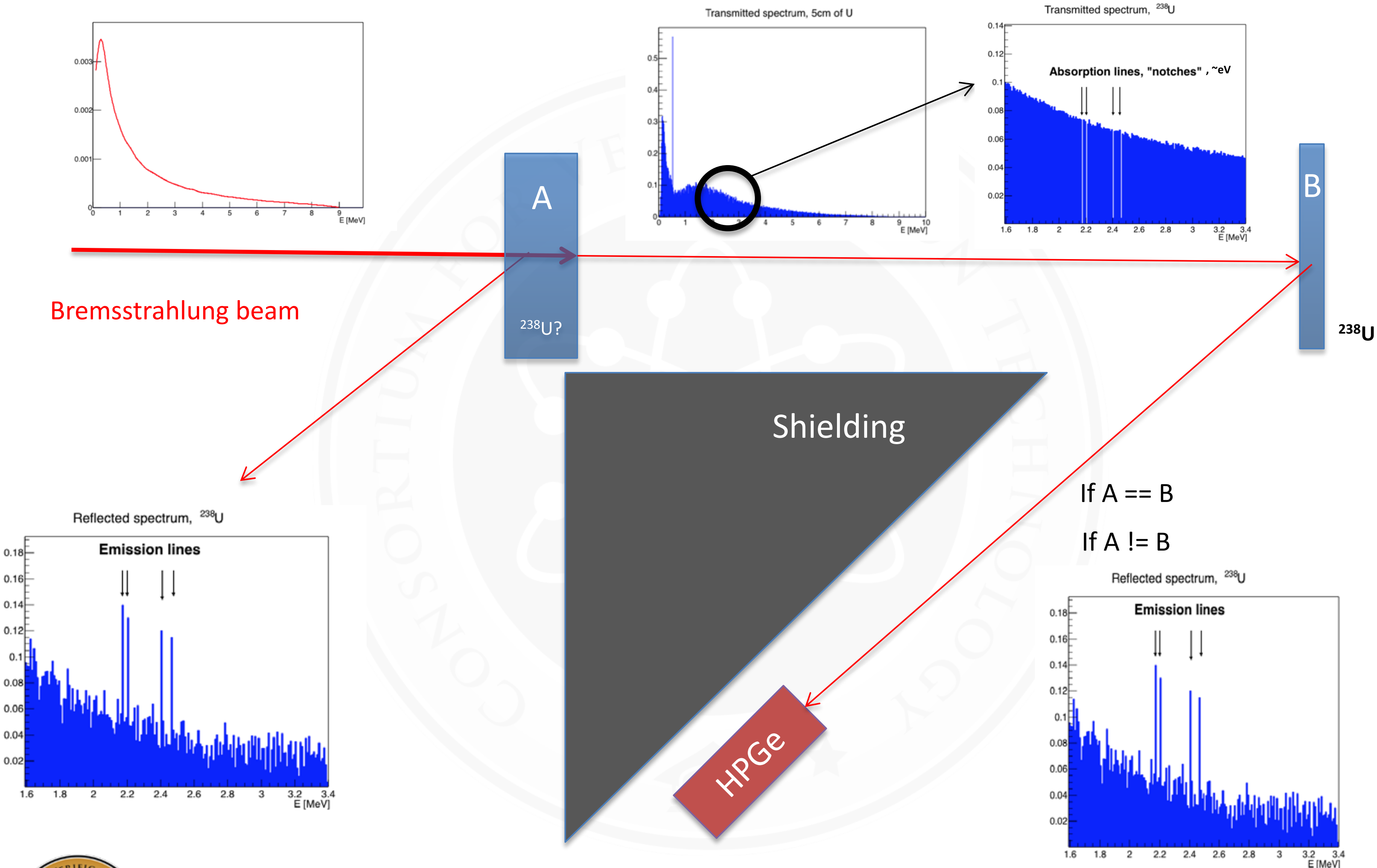


- Follows Breit-Wigner distribution for a resonance, widths of ~10meV
- Thermal Doppler effects widen to $\Delta = E_c \sqrt{kT / M} \sim eV$

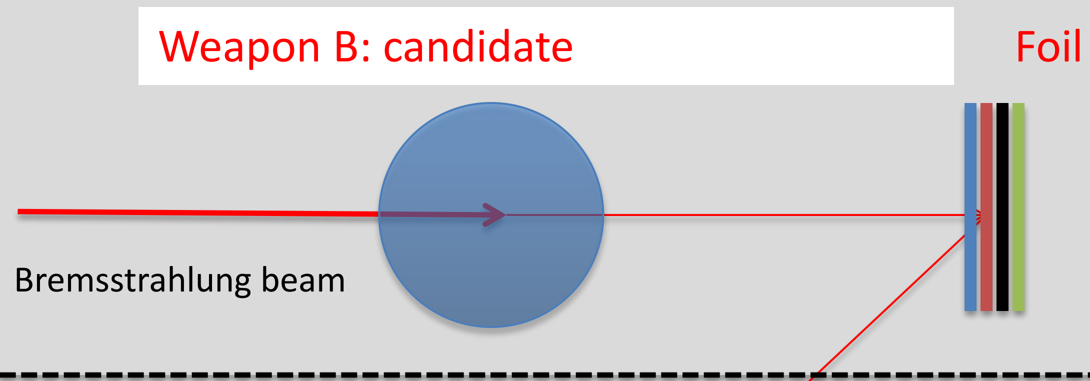
$$\sigma(E) = \frac{2J_1+1}{2J_0+1} \frac{1}{4}\lambda_0^2 \frac{\Gamma_0}{\Gamma} \frac{\Gamma_i}{\sqrt{\pi}\Delta} \exp\{-[(E-E_r)/\Delta]^2\}$$

J. C. PALATHINGAL and M, L. WIEDENBECK, 1969

NRF: backscattered and reference foil

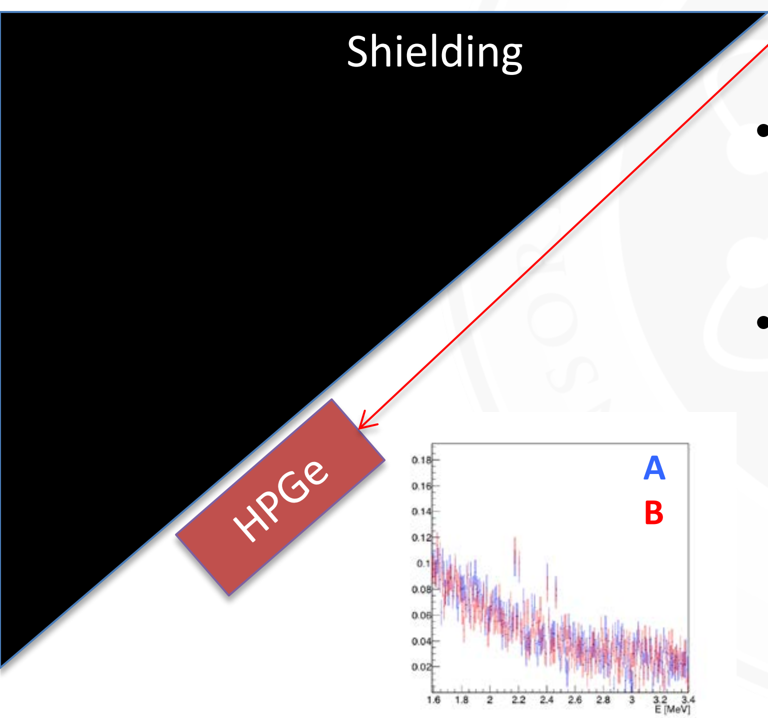


NRF Weapon authentication: ConOps



Everything classified by the host

Everything open



- <u>Zero Knowledge:</u>
  - No direct data from the weapon itself
  - For *all* acquired spectra: $S_{NRF} = (Weapon) \otimes (Foil)$
  - Impossible to extract (Weapon)
- <u>Soundness and completeness:</u>
  - Authenticated template A -- acquire S_{NRF}(A)
  - Candidate weapon B -- acquire S_{NRF}(B)
  - Perform a spectral comparison
    - Kolmogorov test
    - χ^2 test, e.g. P(chi2>83,ndf=180)=0.99
    - …
  - Verify that the weapons are identical to within a confidence using likelihood ratio tests: $F = \log_{10} \frac{P(diversion \mid data)}{P(null \mid data)}$

Going Forward: Policy Research

- What characteristics of the weapon really matter?
- How much resolution is tolerable?
- Political restraints on verification protocol

Going Forward: Nuclear Science

- Geant4 simulations of (U, Pu, C, Fe, Be)
- Analytic validation of G4NRF class (Jordan *et al.*)
- Analyze notch refill from Compton scattering. How does it affect analyzing power?
- Simulate operational scenarios, determine detection probability and false positive prob:
  - Two identical weapons. What's the FP of the decision algorithm?
  - Introduce a difference Δ. What's the dependence of DP on Δ?
  - What's the optimal foil composition?
- Test various decision algorithms for detecting a diversion and clearing a null

Going Forward: Experimental Work

- Build a prototype
  - 4 HPGe detectors
  - 3MeV Van de Graaf at MIT HVRL, possibly another CW machine?
- Acquire NRF data,
  - Perform data driven validations of G4NRF module
  - use that to perform basic validation of the NRF in Geant4.
- Perform tests of the ConOps with various surrogates, e.g. ~100 g/cm^2 of ^{238}U.