Ezra Engel, Areg Danagoulian

Email: aregjan@mit.edu
Twitter: @varpetareg

Experiments show that Epithermal Neutron beams can be used for *Physically Cryptographic Warhead Verification*

"Trust, but **verify**!", „ Доверяй, но **проверяй**! " Но как? How? Ինչպե՞ս:

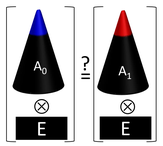
Template Verification

- Acquire an authentic warhead – "golden copy"
- Golden copy is the basis of all comparisons
- Acquire a candidate warhead
- Perform a comparison
  - No information can leak
    - → use **physical encryption (no computers)**
  - Verify that the two objects are identical
    - → use an isotope-sensitive process, **nuclear resonances**
- → candidate becomes authentic.

Analogy with underdefined system of equations:

X + Y = 10
(encrypting filter; "golden copy" weapon)

X' + Y = 10
("candidate weapon")



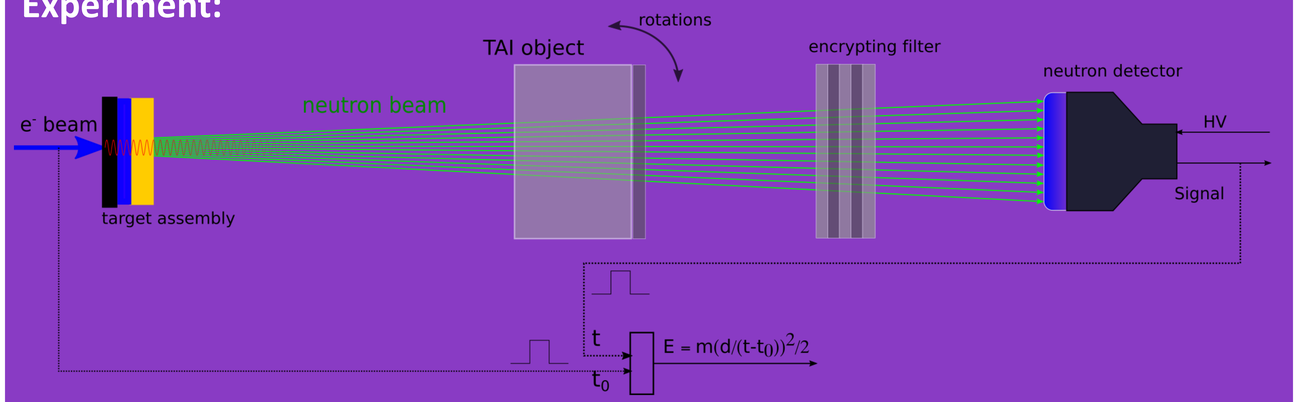
Conclusion:

X' - **X** = 0. ⟹ **X' = X**

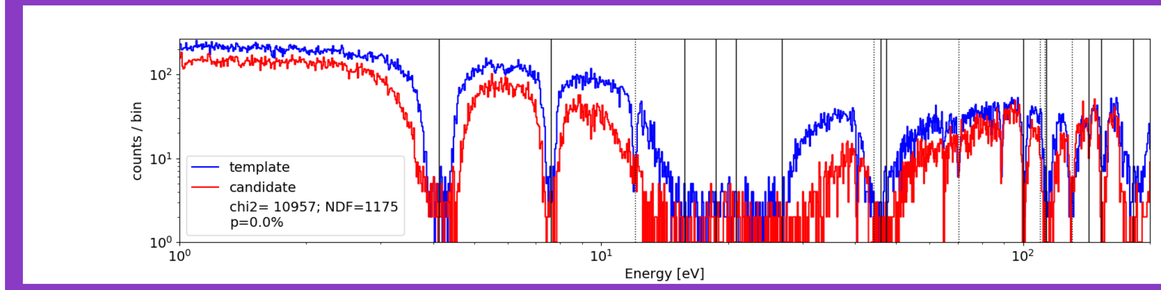
Information Security: X can be anything between 0 to 10.

The technique is very **sensitive to differences** between two objects, **enabling verification**. It is **INsensitive** to the object mass/geometry/enrichment, **protecting secrets**.

Experiment:



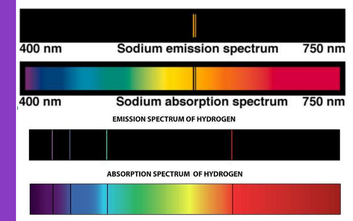
Results – clear difference between an honest and a cheat:

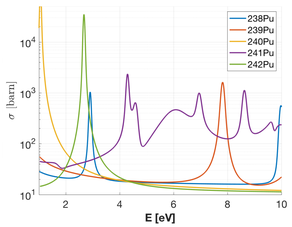


RESONANCES

Nuclear resonances are like atomic transitions / fluorescence, except at 1mln times higher energies.

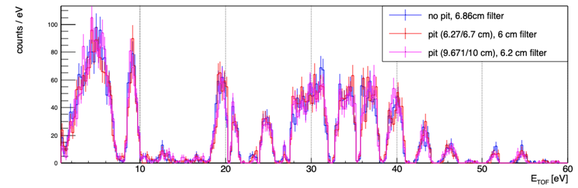
Analogy: atomic fluorescence



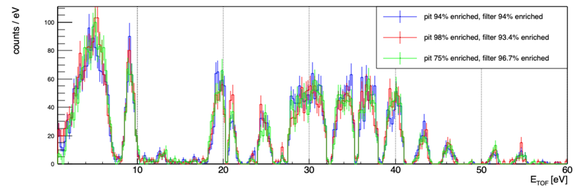


INFORMATION SECURITY

Simulations show that no information unique to the weapon component can be inferred.



Identical signals. Inspector can't distinguish between **no pit** and **impossible pit** (>> critical mass!)



Identical signals. Inspector can't distinguish between **75%** and **98%.**

CONCLUSIONS

We **CANNOT** infer the object content.
We **CAN** verify that the object is identical to the "golden copy."

→The object *must* be authentic
→No secrets revealed

Take a picture to **download** the **full paper, OR to learn about us**