HIDDEN IN PLAIN SIGHT
CAN CRYPTOGRAPHY HELP CRACK THE NEXT GENERATION OF NUCLEAR ARMS-CONTROL TREATIES?

Alexander Glaser and Sébastien Philippe
Princeton University
Ruhr-Universität Bochum, November 17, 2017
BACKGROUND
There remain about 15,000 nuclear weapons in the world today.

Hans Kristensen and Robert Norris, Nuclear Notebook, Federation of American Scientists and thebulletin.org/nuclear-notebook-multimedia
Even a “limited” nuclear war has global environmental consequences.

Smoke from a regional nuclear war between India and Pakistan.

A modern nuclear weapon has a destructive power tens to hundreds of times greater than the Hiroshima bomb.

New York City
A 200-kiloton nuclear explosion would immediately kill more than 1,300,000 people in New York City and the surrounding areas. Fallout effects would significantly increase this number.
### NUCLEAR WEAPON STOCKPILES, 2017

(ONLY ABOUT 20% ARE CAPTURED BY ARMS-CONTROL AGREEMENTS)

<table>
<thead>
<tr>
<th>Country</th>
<th>Total warheads (peak)</th>
<th>Total warheads (2017)</th>
<th>Deployed warheads (strategic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>31,255</td>
<td>~ 6,800</td>
<td>1,393</td>
</tr>
<tr>
<td>Russia</td>
<td>~ 40,000</td>
<td>~ 7,000</td>
<td>1,561</td>
</tr>
<tr>
<td>France</td>
<td>540</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>500</td>
<td>215</td>
<td></td>
</tr>
<tr>
<td>China</td>
<td></td>
<td>270*</td>
<td></td>
</tr>
<tr>
<td>Israel</td>
<td></td>
<td>80*</td>
<td></td>
</tr>
<tr>
<td>India</td>
<td></td>
<td>110*</td>
<td></td>
</tr>
<tr>
<td>Pakistan</td>
<td></td>
<td>120*</td>
<td></td>
</tr>
<tr>
<td>North Korea</td>
<td></td>
<td>20*</td>
<td></td>
</tr>
</tbody>
</table>

Adapted from Nuclear Notebook, fas.org/issues/nuclear-weapons/status-world-nuclear-forces

*Estimate

New START data as of October 2017
WHAT’S NEXT FOR NUCLEAR ARMS CONTROL?

2015 STATEMENT BY JAMES MATTIS

“\nThe nuclear stockpile must be tended to and fundamental questions must be asked and answered:

• We must clearly establish the role of our nuclear weapons: do they serve solely to deter nuclear war? If so we should say so, and the resulting clarity will help to determine the number we need.
• Is it time to reduce the Triad to a Diad, removing the land-based missiles? This would reduce the false alarm danger.
• Could we re-energize the arms control effort by only counting warheads vice launchers?
• Was the Russian test violating the INF treaty simply a blunder or a change in policy, and what is our appropriate response?”

General James N. Mattis, USMC (Ret.)
Former Commander, United States Central Command

Senate Armed Services Committee
Global Challenges and U.S. National Security Strategy
January 27, 2015
INTERNATIONAL PARTNERSHIP
FOR NUCLEAR DISARMAMENT VERIFICATION

Established in 2015; currently 26 participating countries

Working Group One: “Monitoring and Verification Objectives” (chaired by Italy and the Netherlands)
Working Group Two: “On-Site Inspections” (chaired by Australia and Poland)
Working Group Three: “Technical Challenges and Solutions” (chaired by Sweden and the United States)

www.state.gov/t/avc/ipndv
CONSORTIUM FOR VERIFICATION TECHNOLOGY

Five-year project, funded by U.S. DOE, 13 U.S. universities and 9 national labs, led by U-MICH

Princeton participates in the research thrust on disarmament research (and leads the research thrust of the consortium on policy)
WHAT IS TO BE VERIFIED?
THOUSANDS OF NUCLEAR WEAPONS

ARE CURRENTLY NON-DEPLOYED (i.e., IN RESERVE OR AWAITING DISMANTLEMENT)

W87/Mk-21 Reentry Vehicles in storage, Warren Air Force Base, Cheyenne, Wyoming
Photo courtesy of Paul Shambroom, www.paulshambroom.com
VERIFICATION CHALLENGES OF DEEPER REDUCTIONS

- Establishing confidence in the absence of undeclared stocks or production
- Confirming the authenticity of nuclear warheads
- Verifying numerical limits on declared nuclear warheads
- Monitoring nuclear warheads in storage
WHY ARE WARHEAD INSPECTIONS SO HARD?

(AS SEEN FROM INSPECTOR’S PERSPECTIVE)

**VERY LITTLE (IF ANY) INFORMATION ABOUT THE INSPECTED ITEM CAN BE REVEALED**

Some information may be shared in advance, but no additional information during inspection

**ADVERSARY/COMPETITOR HAS (DE FACTO) INFINITE RESOURCES**

**ADVERSARY/COMPETITOR MAY BE EXTREMELY MOTIVATED (TO DECEIVE INSPECTOR)**

Stakes are very high (especially when the number of weapons drops below ~1,000)

**HOST HAS LAST OWNERSHIP OF INSPECTION SYSTEM BEFORE THE MEASUREMENT**

(and inspector never again has access to system after the measurement is complete)
CONFIRMING THE AUTHENTICITY OF WARHEADS

(THE ORTHODOX APPROACH)
VERIFICATION CHALLENGES OF DEEP REDUCTIONS

Confirming the authenticity of nuclear warheads
NUCLEAR WEAPONS HAVE UNIQUE SIGNATURES
BUT THEY ARE SENSITIVE AND CANNOT BE REVEALED TO INSPECTORS

U.S. Scientists on a Soviet Cruiser in the Black Sea, 1989
NUCLEAR WARHEAD VERIFICATION

KEY CONCEPTS OF (PROPOSED) SYSTEMS

ATTRIBUTE APPROACH
Confirming selected characteristics of an object in classified form (for example, the presence/mass of plutonium)

TEMPLATE APPROACH
Comparing the radiation signature from the inspected item with a reference item ("golden warhead") of the same type

INFORMATION BARRIERS
Technologies and procedures that prevent the release of sensitive nuclear information (generally needed for both approaches)
THE ORTHODOX APPROACH

25 YEARS OF R&D ... BUT SO FAR NO WINNING TECHNOLOGY OR DESIGN

Fundamental challenge: How can information barriers simultaneously be authenticated and certified, i.e., trusted by inspector team and host team at the same time?
HARDWARE TROJANS

STEALTHY MODIFICATIONS TO AN INTEGRATED CIRCUIT THAT ADD OR REMOVE FUNCTIONALITIES

CAN YOU TRUST THIS CHIP?

Does the hardware meet the design specifications?
Does it perform as intended?

Insertion of trojan is possible at every stage of the product cycle in particular, during design, manufacturing, assembly, and shipping (supply chain)

HARDWARE VERIFICATION CHALLENGES

Reproducibility is difficult; trojans can be triggered by aging mechanisms or environmental conditions; extremely hard for inspector to reproduce

Below transistor level: Terra Incognita; so far no solutions

ONE (BIG) ISSUE REMAINS
NO POST-MEASUREMENT INSPECTION OF EQUIPMENT

After all these years, no one has yet demonstrated either an attribute or template type system using a classified test object in such a way that specialists from the inspecting country can then [i.e., after the measurement] thoroughly examine and proof the measurement equipment.”

James Fuller, October 2012
WHAT TO DO WHEN THERE REMAIN ENDURING CONCERNS ABOUT INFORMATION SECURITY

CONTINUE IMPROVING TECHNOLOGIES AND APPROACHES
Work on information barriers with a particular focus on certification and authentication; in particular, identify joint hardware and software development platforms

REINVENT THE PROBLEM: NEVER ACQUIRE SENSITIVE INFORMATION TO BEGIN WITH
Explore radically different verification approaches; for example, consider zero-knowledge protocols and develop alternatives to onsite inspections at certain sensitive facilities

REVEAL THE SECRET
Requirement to protect sensitive information is typically the main reason for complexity of verification approaches; for example, mass of fissile material in a nuclear weapon

Source: Author (top and bottom), Christian Zenger (middle)
IMPROVING TECHNOLOGIES & APPROACHES

INFORMATION BARRIER
EXPERIMENTAL &
VINTAGE VERIFICATION

INFORMATION BARRIER EXPERIMENTAL

A PROTOTYPING PLATFORM FOR HARDWARE AND SOFTWARE CHALLENGES?

M. Kütt, M. Göttsche, and A. Glaser, “Information Barrier Experimental,” Measurement, 114, 2018

“VINTAGE VERIFICATION”

SIMPLE, WIDELY AVAILABLE, WELL UNDERSTOOD ELECTRONICS (AND NEVER INTENDED FOR USE IN SECURITY APPLICATIONS)

(Talk at 34c3, December 2017)
ZERO-KNOWLEDGE NUCLEAR WARHEAD CONFIRMATION

REINVENTING THE PROBLEM # EXAMPLE 1
PHYSICAL ZERO-KNOWLEDGE PROOFS

CAN WE SHOW TWO OBJECTS ARE IDENTICAL WITHOUT LEARNING WHAT THEY ARE?

Bob wants to prove to Alice that two objects are “identical” in a way that Alice gains no new knowledge about the objects themselves.
14 MeV neutron generator
(Thermo Scientific P 385)

Collimator

Collimator slot

Test object

Detector array
S. Philippe, R. J. Goldston, A. Glaser, F. d’Errico, “A physical zero-knowledge object-comparison system for nuclear warhead verification,” *Nature Communications*, 7, September 2016, [www.nature.com/articles/ncomms12890](http://www.nature.com/articles/ncomms12890)
SUPERHEATED EMULSIONS AS PUF-DETECTORS

OPEN PATH FOR TRUSTED MEASUREMENTS

AVOID DETECTOR-SIDE ELECTRONICS

Superheated emulsions are designed to be insensitive to $\gamma$-radiation and sensitive to neutrons with energy $E_n > E_{\text{min}}$.

Tailor-made by Francesco d’Errico Research Group, Yale University.

HAVE PROPERTIES OF AN OPTICAL PHYSICALLY UNCLONABLE FUNCTION

Could allow host to review the data before the inspector sees it while giving the inspector confidence the data was not tampered with.

First experimental results are promising: detectors are unique objects, physically unclonable, and challenge response pairs are sensitive to neutron interaction.

Source: Authors (Top: A. Glaser.; Bottom: Experimental Set-up, S. Philippe)
CONFIRMING NUMERICAL LIMITS ON NUCLEAR WARHEADS
VERIFICATION CHALLENGES OF DEEP REDUCTIONS

Verifying numerical limits on declared nuclear warheads
TAGGING

TRANSFORMING A “NUMERICAL LIMIT” INTO A “BAN ON UNTAGGED ITEMS”


Source: www.automoblog.net
VERIFYING NUMERICAL LIMITS OF DECLARED NUCLEAR WARHEADS

WARHEAD TAGGING OPTIONS

AN ALTERNATIVE TO TAGGING: CRYPTOGRAPHIC ESCROW

ITEM 999: b86d553666858d3c611884207c40b2eb3d9a3ac94a8cae9e4cd34deaa95ff589

m_0 = {152441ff1a5b9f3f},
{fe2b9cba3ef8d73e},
{"type: w99", "site: air base 001", "status: stored"},
{5a85ac7ef688d9aceec32b1ef3d5779add02989fa8161f65c86a306e2ad57e07}

digest_0 = sha256(m_0)

m_1 = {db91dc3900328ca2},
{"serial: w99xyz1234", "pu: 4.000 94.000", "u: 15.000 97.000"}

digest_1 = sha256(m_1)

Shown commitments (generated with the SHA-256 hash function) are for illustration purposes only; actual messages and digests may use a different commitment scheme.
WAY FORWARD & NEXT STEPS

PREPARING FOR DEEPER REDUCTIONS AND MULTILATERAL NUCLEAR ARMS CONTROL

TAKING INFORMATION SECURITY SERIOUSLY

Jointly develop and demonstrate methods to confirm numerical limits on nuclear warheads and confirm their authenticity

Focus initially on non-intrusive approaches that are acceptable to all participants (but can accommodate “upgrades”)

THINKING OUTSIDE THE BOX

- Proof of knowledge and trusted sensors
- Next-generation data exchange (cryptographic escrow, blockchains)
- Involve broader crypto-community (hackathons)