SAND2015-5704C

Zero Knowledge Protocol: Challenges and Opportunities

Peter Marleau

Erik Brubaker, Nathan Hilton, Michael McDaniel, Richard Schroeppel, Kevin Seager, and Sharon DeLand

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Approved for unlimited release, SAND2015-C

Sandia National Laboratories

Zero Knowledge Protocol for warhead verification?

ARTICLE

doi:10.1038/nature13457

A zero-knowledge protocol for nuclear warhead verification

Alexander Glaser[1], Boaz Barak[2] & Robert J. Goldston[3]

The role of the inspector:

- More crypto-procedural part of the protocol.
- Last minute choice increases confidence in the measurement.

The verification measurement:

- Zero-knowledge in the result, but less ZKP-like in procedure.
- An interesting take on template measurements with a physical information barrier.

Outline

- What is ZKP
  - Is there an Arms Control equivalent to cryptographic ZKP?
- Separable concepts: role of the inspector vs. physical template matching
- Role of the inspector – confidence by participation
  - Problems? – fault tolerance and third parties.
- Physical template matching – confidence without information leakage
  - Problems? – Information loss in an imperfect world.
- The authenticated standard
  - How do we authenticate the authenticated standard?
- Some ideas:
  1. Role of the inspector in choosing the authenticated standard – Choosing from deployment. Choosing from items to be tested from host presentation.

Zero Knowledge Protocol – abstracted

Our understanding of a cryptographic implementation

1. "Host" wishes to offer verification to one or more parties that they hold some information without leaking any.
2. "Inspector" offers an unknown "key" to be incorporated into a verifiable challenge that can only be successfully completed with the information.
3. "Host" prepares two verification challenges that the "inspector" chooses from.
4. "Host" answers.
5. "Inspector" verifies the accuracy of their response using their "key".
6. Confidence increases with repeated challenges.

Example:

Host – "I know the prime factors of large number N"

Square roots modulo N are easy to calculate with its factors.

- Inspector challenge – "complete a square root mod N".
- Inspector chooses W such that $X = W^2 \pmod N$.

- Host prepares $R^2 \pmod N$ and $XR^2 \pmod N$
- Inspector asks for the square root of one of these numbers.
- Inspector verifies the result using X.

Zero Knowledge Protocol – abstracted

Our understanding of a cryptographic implementation

1. "Host" wishes to offer verification to one or more parties that they hold some information without leaking any.
2. "Inspector" offers an unknown "key" to be incorporated into a verifiable challenge that can only be successfully completed with the information.
3. "Host" prepares two verification challenges that the "inspector" chooses from.
4. "Host" answers.
5. "Inspector" verifies the accuracy of their response using their "key".
6. Confidence increases with repeated challenges.

Example:

Host – "I know the prime factors of large number N"

Square roots modulo N are easy to calculate with its factors.

- Inspector challenge – "complete a square root mod N".
- Inspector chooses W such that $X = W^2 \pmod N$.

- Host prepares $R^2 \pmod N$ and $XR^2 \pmod N$
- Inspector asks for the square root of one of these numbers.
- Inspector verifies the result using X.

Sandia National Laboratories

Zero Knowledge Protocol – high level

Our understanding of what has been proposed for Arms Control

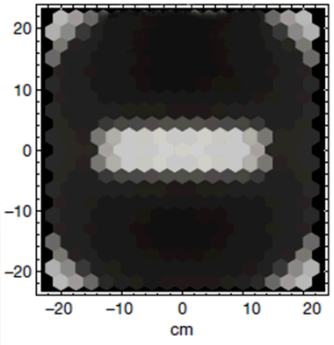
1. Selection of the authenticated standard "template" (optional?)
2. A maximum number of counts is agreed to (presumes tech).
3. Host prepares "preloads" (inverse of positive measurements).
4. Host presents declarations and equipment preloaded with padded counts.
5. Inspector pairs objects with equipment.
6. Host makes measurement.
7. Inspector verifies "flat" result.
8. Inspector verifies equipment functionality.
9. Repeat.

"This is a warhead"

W

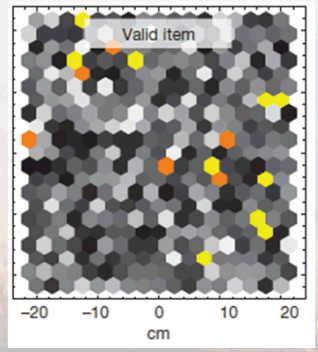
N_{max}

$P = W^{-1}$



$\{I_1, I_2, I_3, W\}$

$P * I_2 = (N_{max})$



Images shamelessly taken from:
Glaser, Barak, and Goldston, "A zero-knowledge protocol for nuclear warhead verification", doi:10.1038/nature 134557

Sandia National Laboratories

Zero Knowledge Protocol – Advantages

Inspector choice:

1. The inspector's last minute choice among items and preloads lends confidence that all items presented are identical.

2. This confidence increases with repeated measurements.

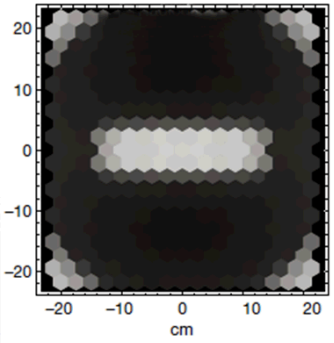
3. If W is present, then the inspector is also confident that they are all warheads.

"This is a warhead"

W

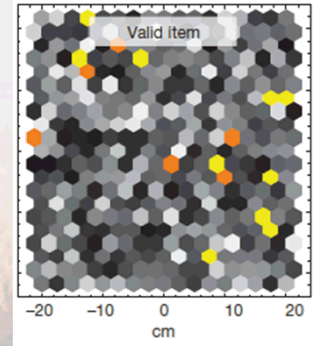
N_{max}

$P = W^{-1}$



$\{I_1, I_2, I_3, W\}$

$P * I_2 = (N_{max})$



Images shamelessly taken from:
Glaser, Barak, and Goldston, "A zero-knowledge protocol for nuclear warhead verification", doi:10.1038/nature 134557

Zero Knowledge Protocol – Advantages

Measurement methodology:

1. Essentially a template based measurement, but the "template" is an inverse such that a positive comparison results in unity.

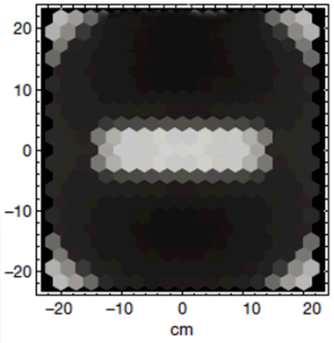
2. The preload is a physical change in the instrument. The information barrier can therefore be physical.

3. A positive measurement leaves the instrument in a verifiable state.

"This is a warhead"

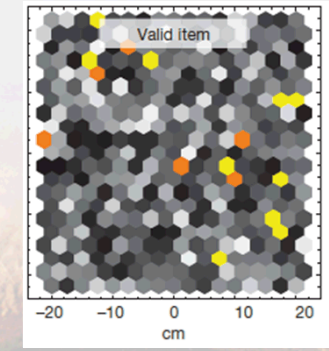
W

N_{max}



$P = W^{-1}$

$\{I_1, I_2, I_3, W\}$



$P * I_2 = (N_{max})$

Images shamelessly taken from:
Glaser, Barak, and Goldston, "A zero-knowledge protocol for nuclear warhead verification", doi:10.1038/nature 134557

Sandia National Laboratories

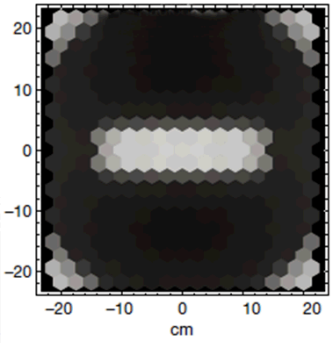
Where's the challenge?

- **In the warhead verification example it was perceived that there is no unknown challenge that leaves the inspector with a verifiable "key" (K).**
- **Each challenge is identical.**
- **The host owns everything except this choice.**

"This is a warhead"

W

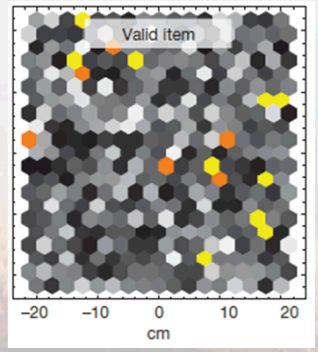
N_{max}



$P = W^{-1}$

$\{I_1, I_2, I_3, W\}$

$P * I_2 = (N_{max})$



Images shamelessly taken from:
Glaser, Barak, and Goldston, "A zero-knowledge protocol for nuclear warhead verification", doi:10.1038/nature 134557

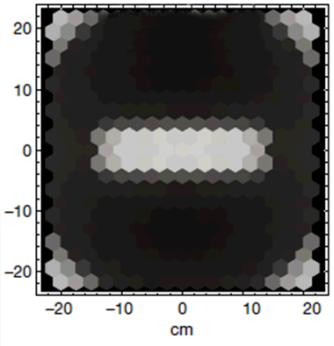
What about a true negative?

- **Can the inspector add something here?**

"This is a warhead"

W

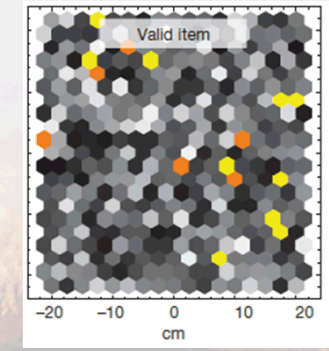
N_{max}



$P = W^{-1}$

$\{I_1, I_2, I_3, W, K\}$

$P * I_2 = (N_{max})$



Images shamelessly taken from:
Glaser, Barak, and Goldston, "A zero-knowledge protocol for nuclear warhead verification", doi:10.1038/nature 134557

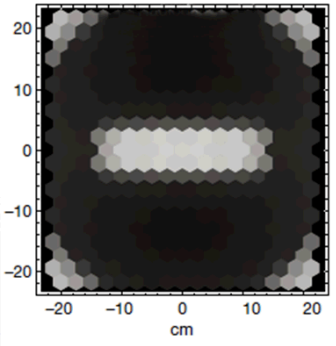
Oops …

- **Not in this implementation, since then your result might look like this.**
- **In fact, any negative result is an information leak.**
- **In fact, an aggregate of positives with a systematic bias can be an information leak.**

"This is a warhead"

W

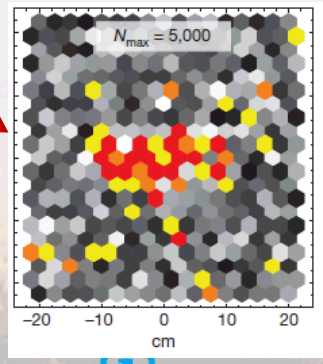
N_{max}



$P = W^{-1}$

$\{I_1, I_2, I_3, W, K\}$

$P * K = (Info)$



Images shamelessly taken from:
Glaser, Barak, and Goldston, "A zero-knowledge protocol for nuclear warhead verification", doi:10.1038/nature 134557

Pre-authenticated standard?

- **Where does this come from?**

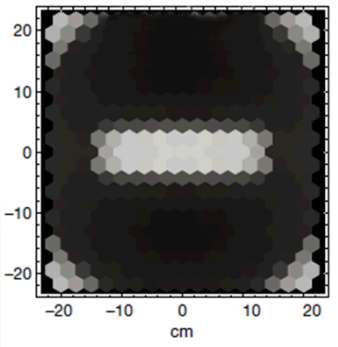
1. **Do we need it?**
2. **Declaration is accepted based on provenance?**
3. **Randomly chosen from deployed items.**
4. **Authenticated by trusted technical means … are we kicking the can?**

→ W

"This is a warhead"

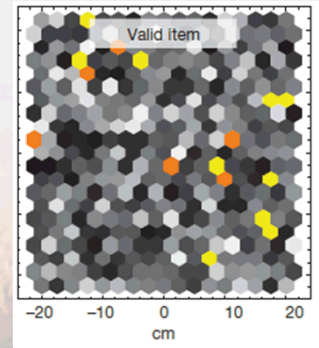
N_{max}

$P = W^{-1}$



$\{I_1, I_2, I_3, W, K\}$

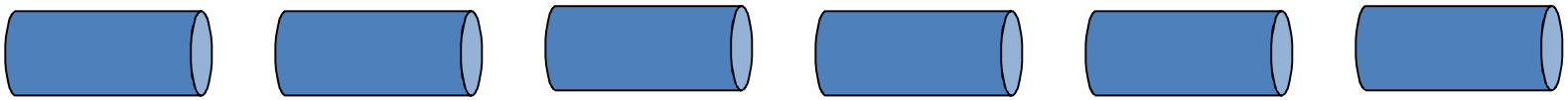
$P * I_2 = (N_{max})$



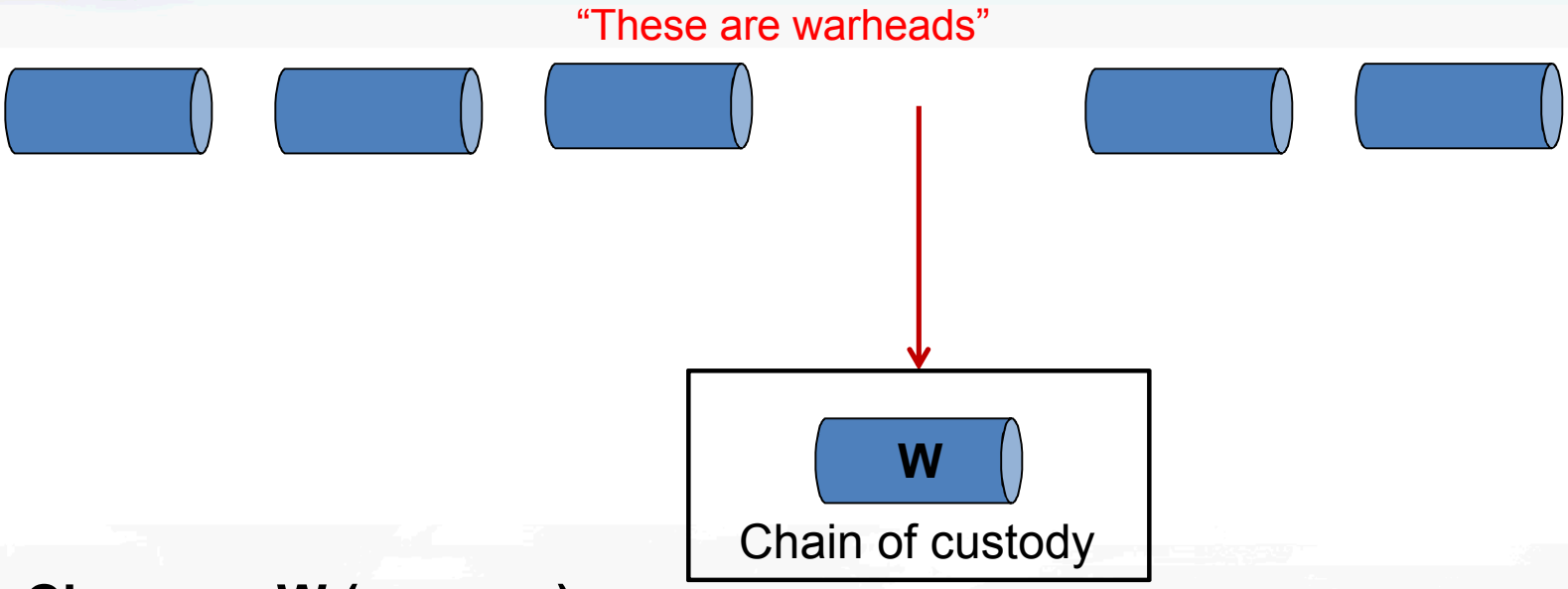
Images shamelessly taken from:
Glaser, Barak, and Goldston, "A zero-knowledge protocol for nuclear warhead verification", doi:10.1038/nature 134557

Initialization …

"These are warheads"



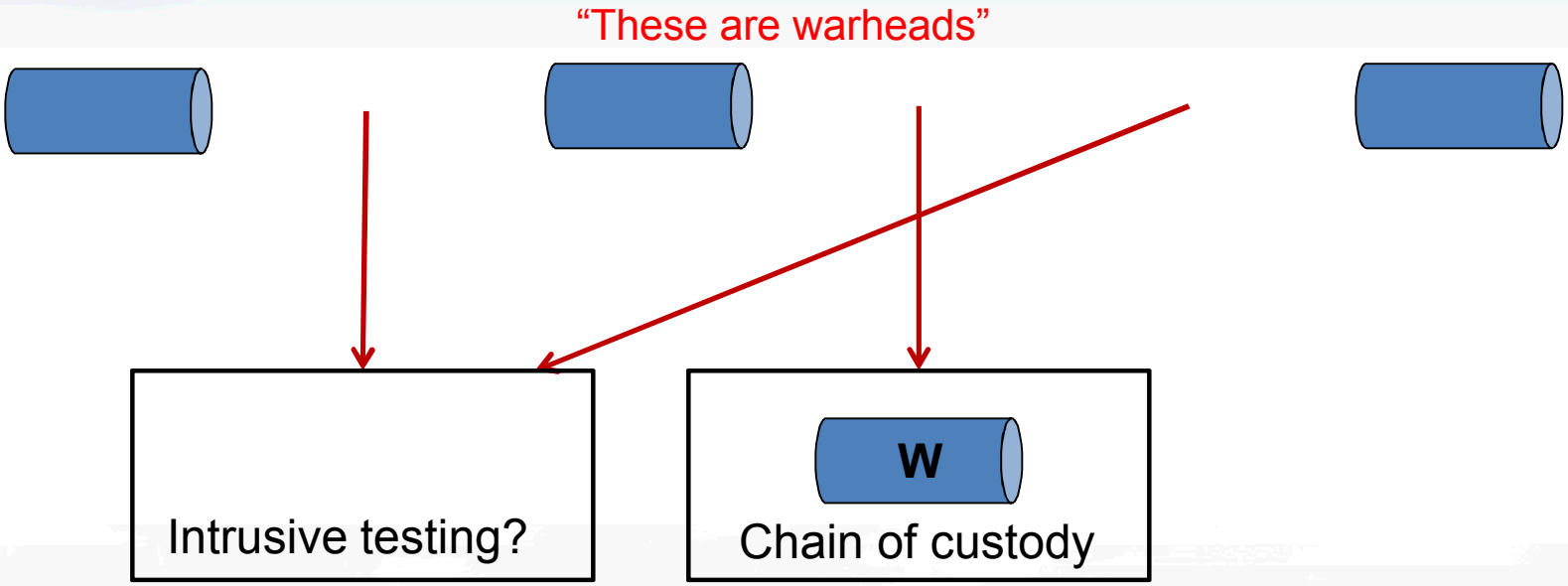
Does selection lend enough confidence?



Choose a W (or more).

- **Accept it.**
- **Authenticate it. But how?**

Do we need something more intrusive?



- **Perhaps testing can include dismantlement. Confirm that explosives will "go boom" …**
- **I now have confidence that my selection is a warhead because it could have been chosen to be tested.**

Conclusions

- ZKP is a useful analogy for the goals of the problem of warhead verification.

- The methodology proposed by Glaser, Barak, and Goldston has two aspects with their own challenges and opportunities:
  1. The role of the inspector's choice in the verification measurements creates confidence that:
     a) All items presented are identical.
     b) All items are identical to warheads (with authenticated standard).
     c) A framework for choosing an authenticated standard?
     d) Authentication of measurement (if true negative can be provided).
  2. A measurement against an inverse "template" offers:
     a) A NULL positive.
     b) A framework for a physical information barrier.