

Practical Implementation of a Zero Knowledge Protocol for Warhead Verification

Principal Investigator: Peter Marleau **Supporting Investigators:** Rebecca Krentz-Wee, Patricia Schuster

Abstract

We constructed and demonstrated a warhead confirmation system using two-dimensional time-encoded imaging (2D-TEI) to provide an authenticatable option for confirmation measurements. It is a physical implementation of a zero knowledge protocol (ZKP), which has intrinsic protection of sensitive information. The 2D-TEI mask modulates the detection rate such that it is constant if and only if two objects are identical. This means that a monitoring party could be allowed full access to the system before, during, and after confirmation without risk of leaking sensitive information.

Goals, Objectives, and Deliverables

- Goal: to address the need for the ability to classify warheads by type while protecting sensitive information
- Objective: to demonstrate a confirmation measurement system which securely and simply utilizes sensitive information without recording it or putting it at risk

Results/Technical Challenges

- Experimentally proved feasibility of new zero knowledge implementation using time-encoded imaging that can be used to confirm two objects are identical
- Objects must be aligned precisely otherwise sensitive information may be at risk
- Need to quantify minimum time needed to confirm objects
- Need to ensure that multiple measurements added together or long measurements don't reveal sensitive information

Planned Accomplishments

- Evaluate minimum measurement times for the existing system to successfully discriminate between items of different sizes and shapes in a series parametric studies
- Develop algorithms that provide metrics that can be sequentially update that may enable confirmation in real-time
- Characterize the alignment precision of the existing system and evaluate its impact on discrimination task performance
- Design a more compact system for gamma-ray imaging in collaboration with University of Michigan (Patricia Schuster)

Research Team

Principal Investigator Contact Information:

- Peter Marleau
- Sandia National Labs
- pmarlea@sandia.gov
- (925) 294-3329

Supporting Investigators:

- Rebecca Krentz-Wee, UC-Berkeley, NSSC
- Patricia Schuster, University of Michigan, CVT affiliate
- NSSC—Nuclear Science & Security Consortium

Notes
