

On-Site Inspections *from* a Distance

The Application of Virtual Proofs of Reality to Nuclear Safeguards And Arms Control Verification

Sébastien Philippe, CVT Associate, Princeton University

2016 Consortium on Verification Technology Workshop, October 19, 2016



CONSORTIUM *for* VERIFICATION TECHNOLOGY



CHALLENGES OF NUCLEAR INSPECTIONS

BACKGROUND



INF inspection. Source: U.S. DOD

TREATIES REQUIRE CREDIBLE INFORMATION-GENERATING MECHANISMS

On-site inspections are a key mechanism for nuclear verification.
Often (if not always) a contentious point of negotiations: what is to be inspected and measured? Frequency of inspections?
(Political & cultural differences also affects the outcome.)



Next Generation Surveillance System. Source: IAEA

FINDING ACCEPTABLE TECHNICAL SOLUTIONS IS DIFFICULT

Physical measurements in sensitive locations require *trusted* equipment.
Classical approaches to distant remote verification require classical tamper-proof hardware, cryptographic keys and digital signatures.
Requirement of protecting sensitive information.



Rethinking

CHALLENGES OF NUCLEAR INSPECTIONS

BACKGROUND



INF inspection. Source: U.S. DOD

TREATIES REQUIRE CREDIBLE INFORMATION-GENERATING MECHANISMS

On-site inspections are a key mechanism for nuclear verification.

Often (if not always) a contentious point of negotiations: what is to be inspected and measured? Frequency of inspections?

(Political & cultural differences also affects the outcome.)



Next Generation Surveillance System. Source: IAEA

FINDING ACCEPTABLE TECHNICAL SOLUTIONS IS DIFFICULT

Physical measurements in sensitive locations require *trusted* equipment.

Classical approaches to distant remote verification require classical tamper-proof hardware, cryptographic keys and digital signatures.

Requirement of protecting sensitive information.



“Virtual Proofs of Reality offer a way to prove physical statements remotely without using classical tamper-resistant hardware and cryptographic keys.”

How to Construct Virtual Proofs of Reality?



Step 1: Turning Sensors into Physical One-Way Functions



PHYSICAL UNCLONABLE FUNCTIONS (PUFs)

ARE THE PHYSICAL EQUIVALENT OF ONE-WAY FUNCTIONS

$$R = f_{\text{PUF}}(C)$$



Properties

Easy To Evaluate But Hard To Predict
Easy To Manufacture But Hard To Duplicate



PHYSICAL UNCLONABLE FUNCTIONS

CAN BE EITHER ELECTRONIC OR NON-ELECTRONIC

PUF

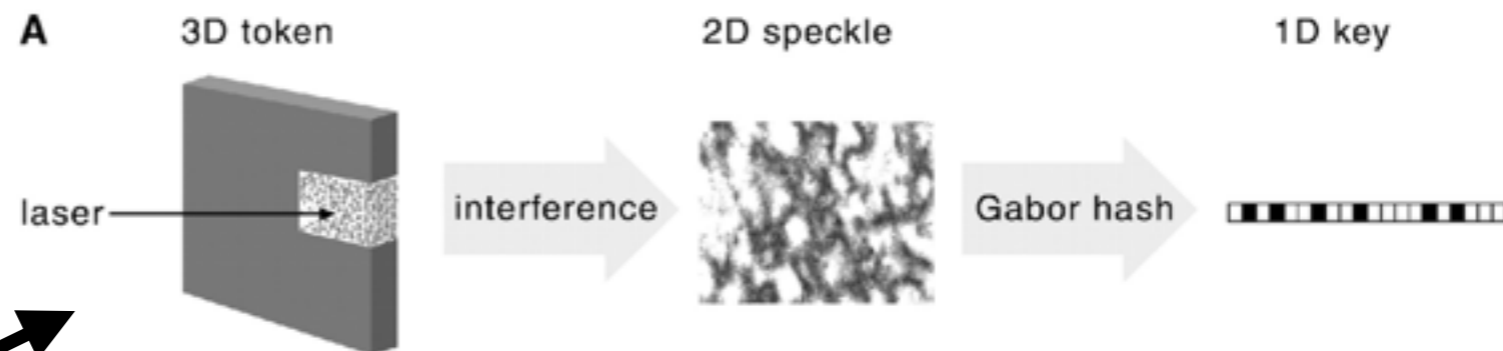
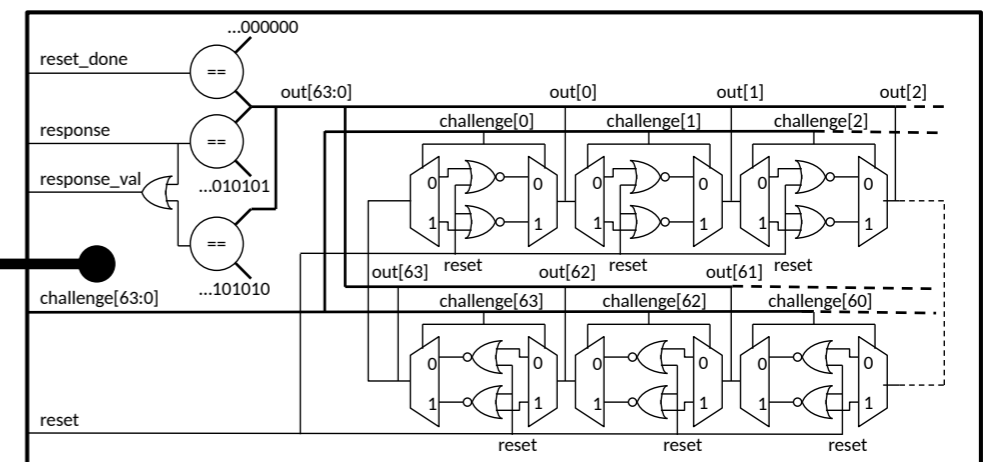
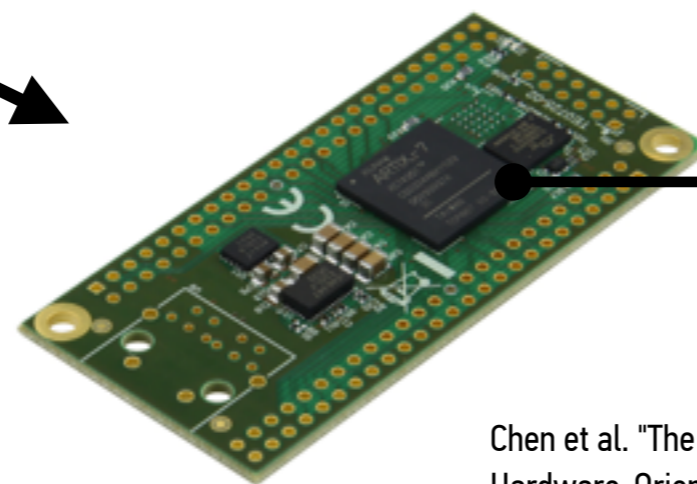


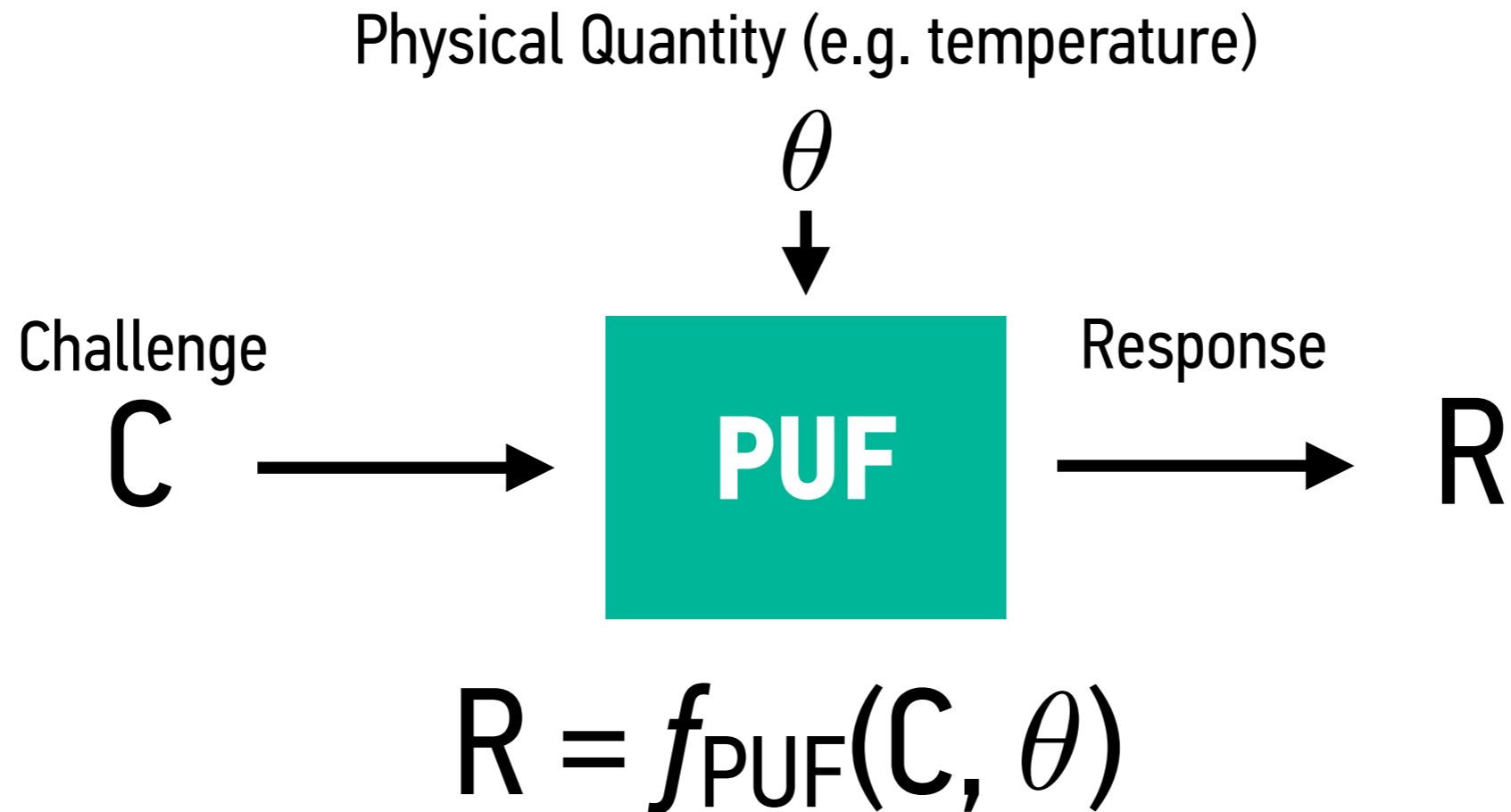
Image: Pappu et al. "Physical One Way Functions," Science, 2002.



Chen et al. "The bistable ring puf: A new architecture for strong physical unclonable functions." Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on. IEEE, 2011.

PHYSICAL UNCLONABLE SENSORS

TURNING PUFs INTO SENSORS - OR *VICE VERSA*



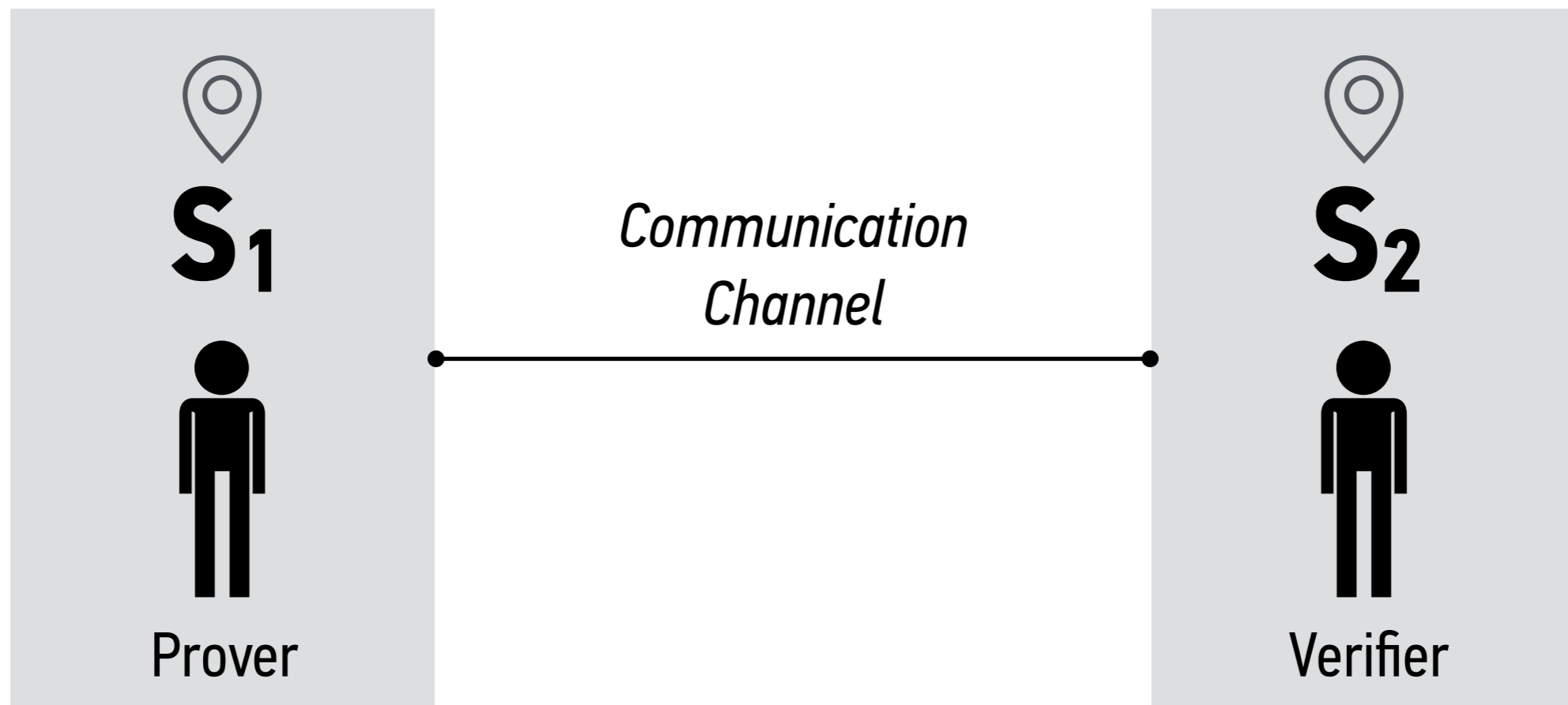
By turning PUFs into Physical Sensors, we can create Challenge-Response pairs dependent on physical quantities

Step 2: Use Sensor-PUFs in an Interactive Protocol



GENERAL ASSUMPTIONS

INTERACTIVE PROOF BETWEEN PROVER AND VERIFIER
IN TWO DIFFERENT LOCATIONS

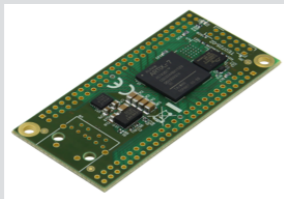


U. Rührmair et al. "Virtual proofs of reality and their physical implementation." 2015 IEEE Symposium on Security and Privacy. IEEE, 2015.

VIRTUAL PROOF PROTOCOL

SET-UP PHASE

A)

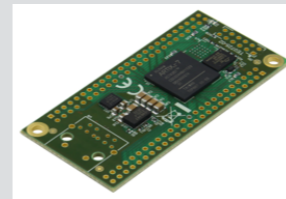


WO_1



WO_2

...



WO_k



S_2

B) For each k prepares $\mathcal{L} = (R_j^i, C_j^i, \Theta_j)$
Where Challenge-Response pairs are constructed
for a given physical quantity Θ_j as

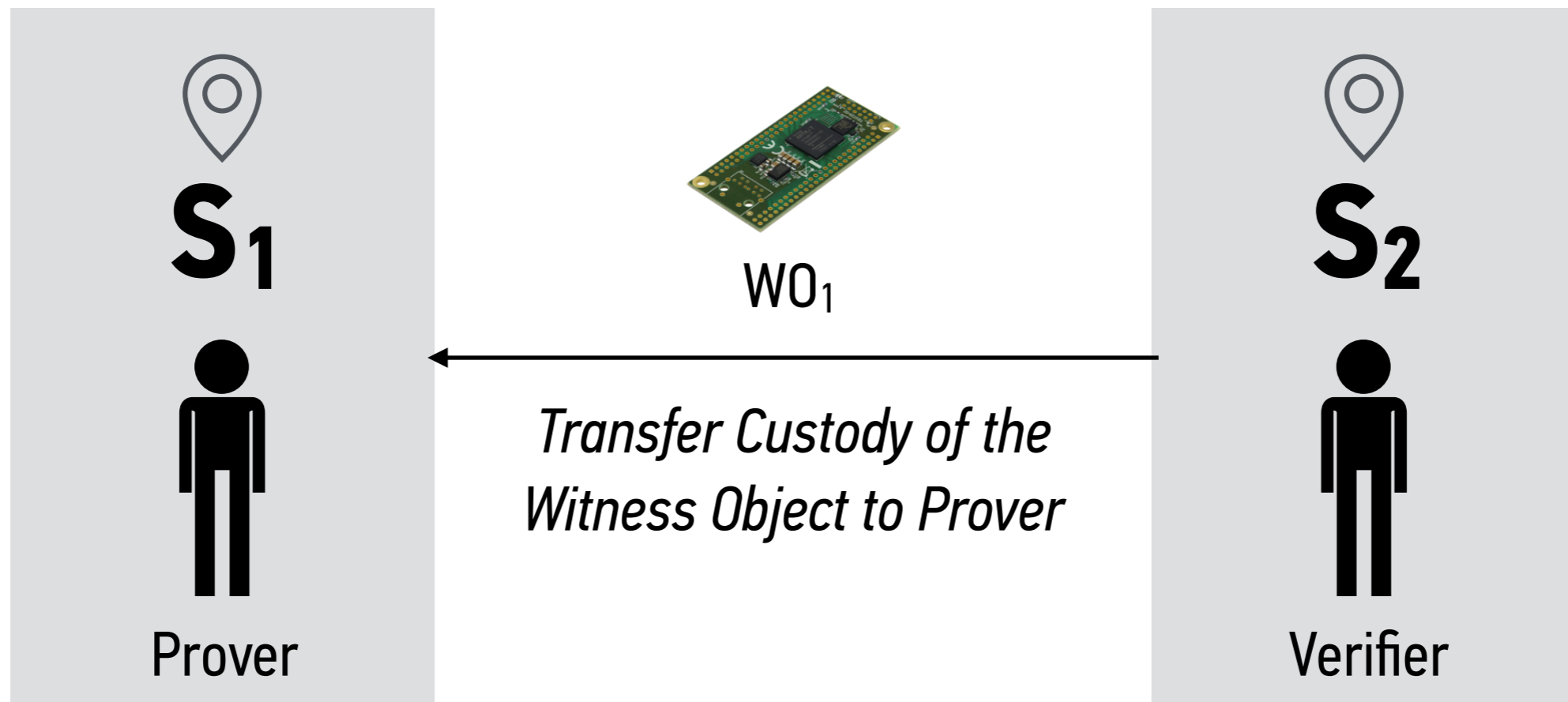
$$R_j^i = F_{WO_k}(C_j^i, \Theta_j)$$



Verifier

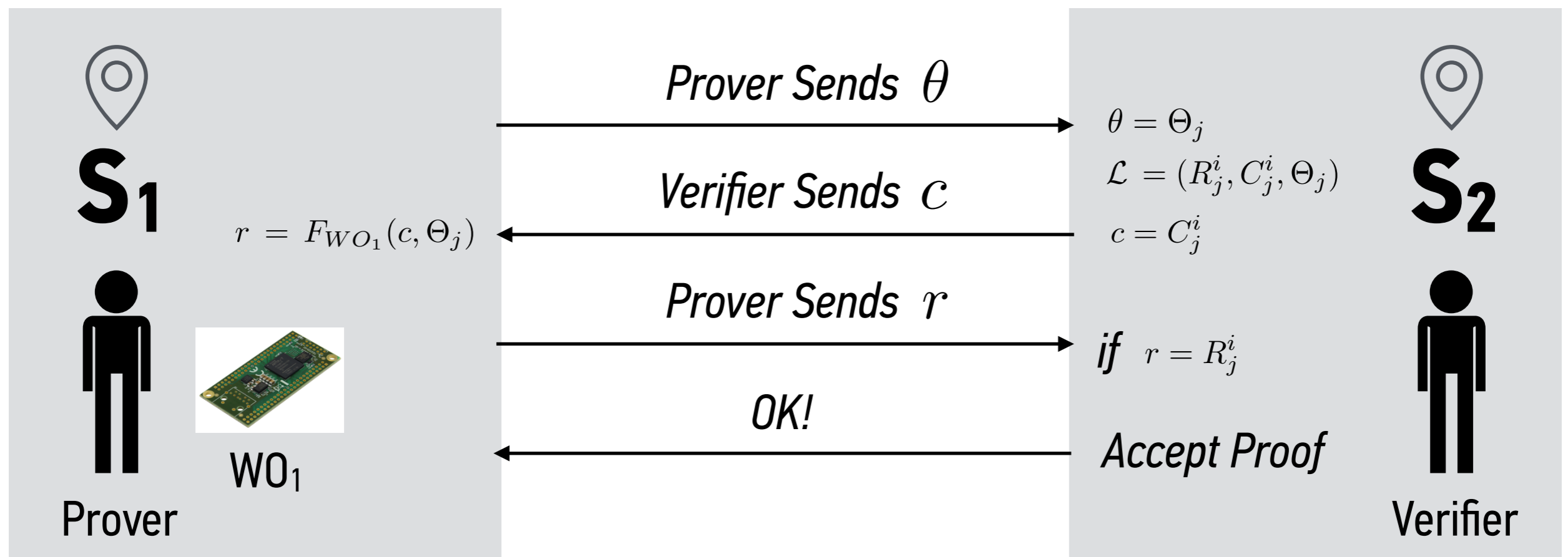
VIRTUAL PROOF PROTOCOL

PROOF PHASE



VIRTUAL PROOF PROTOCOL

PROOF PHASE



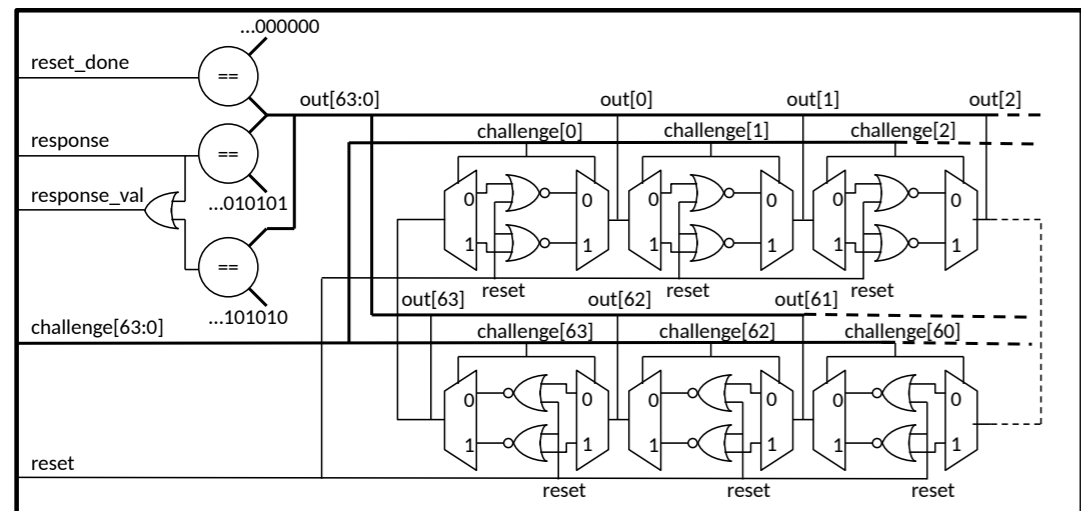
Example 1

A Virtual Proof of Temperature

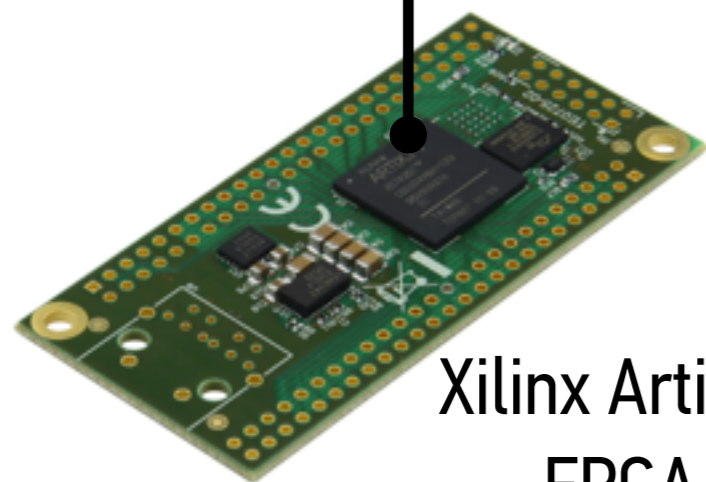


THE BI-STABLE RING PUF

CAN BE TURNED IN A TEMPERATURE SENSOR

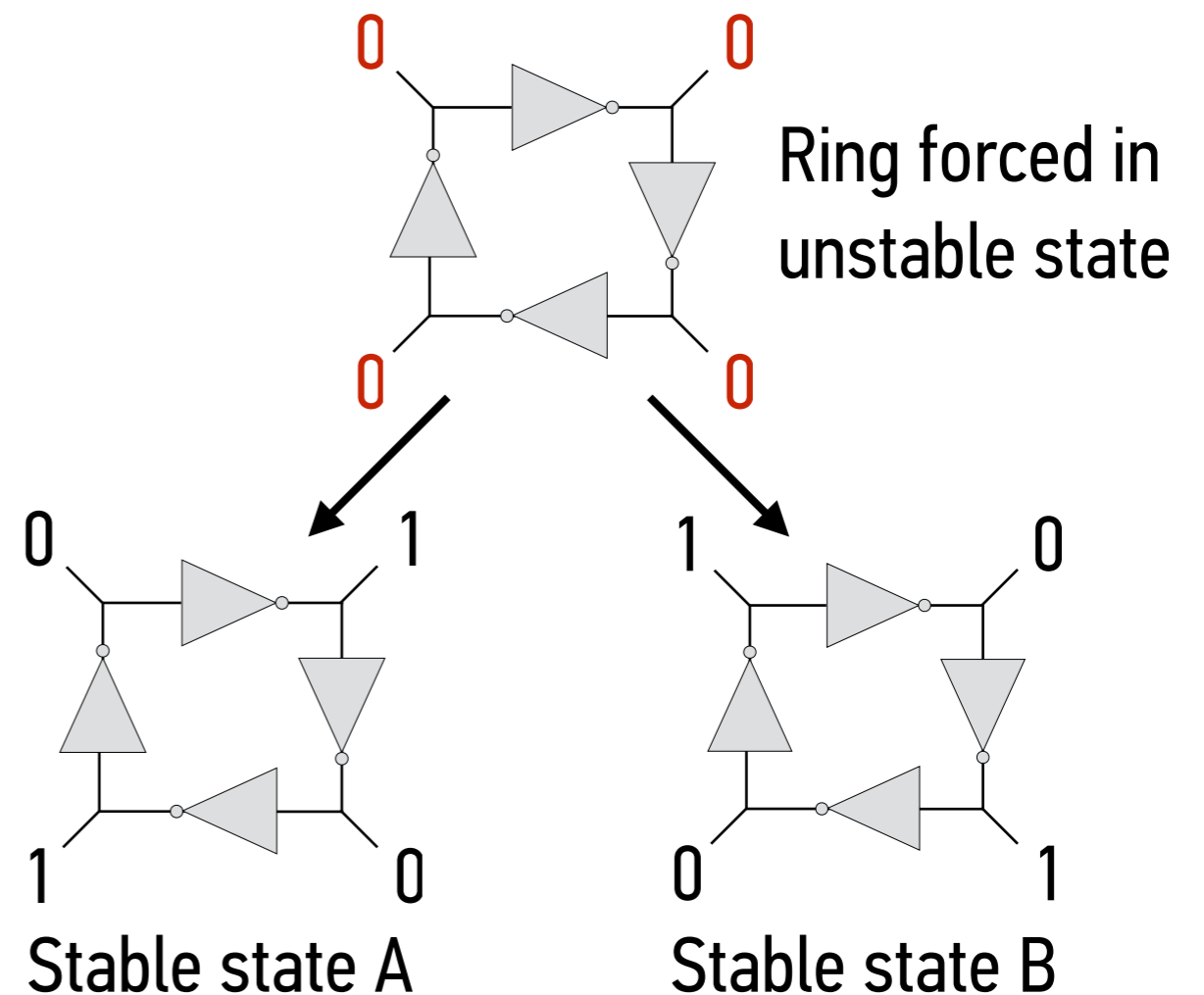


64-bit BR-PUF



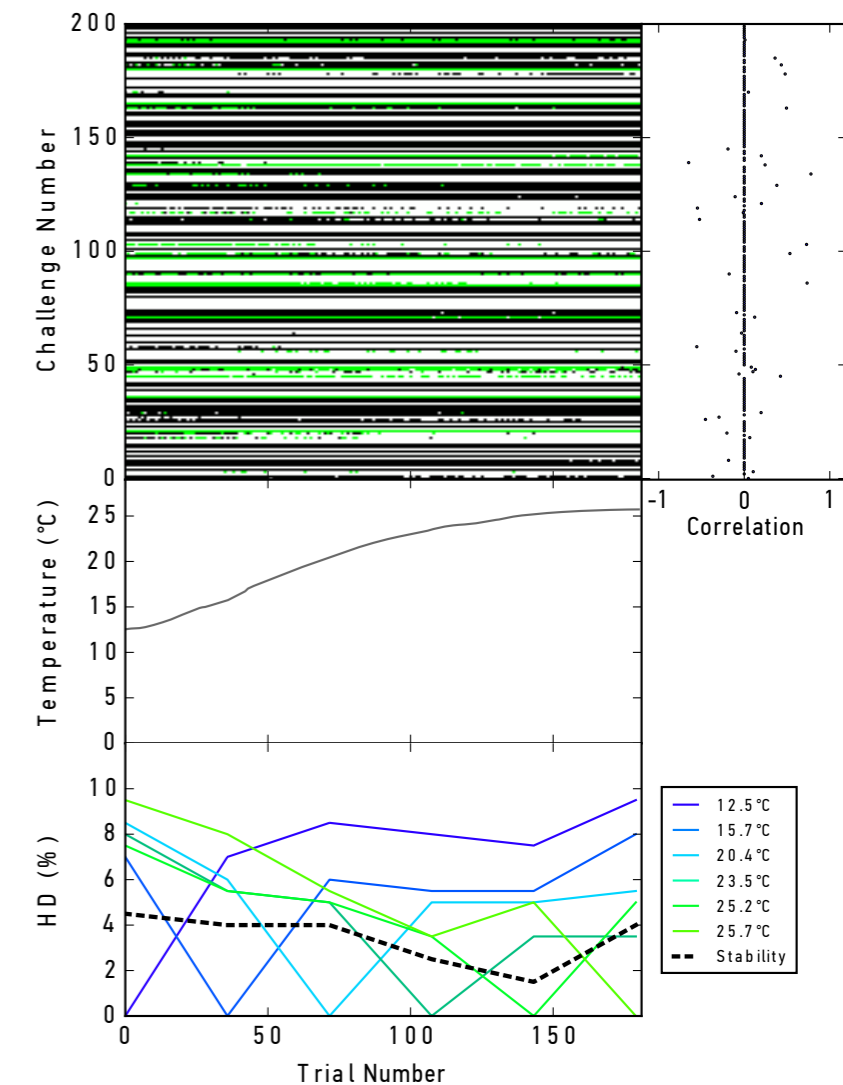
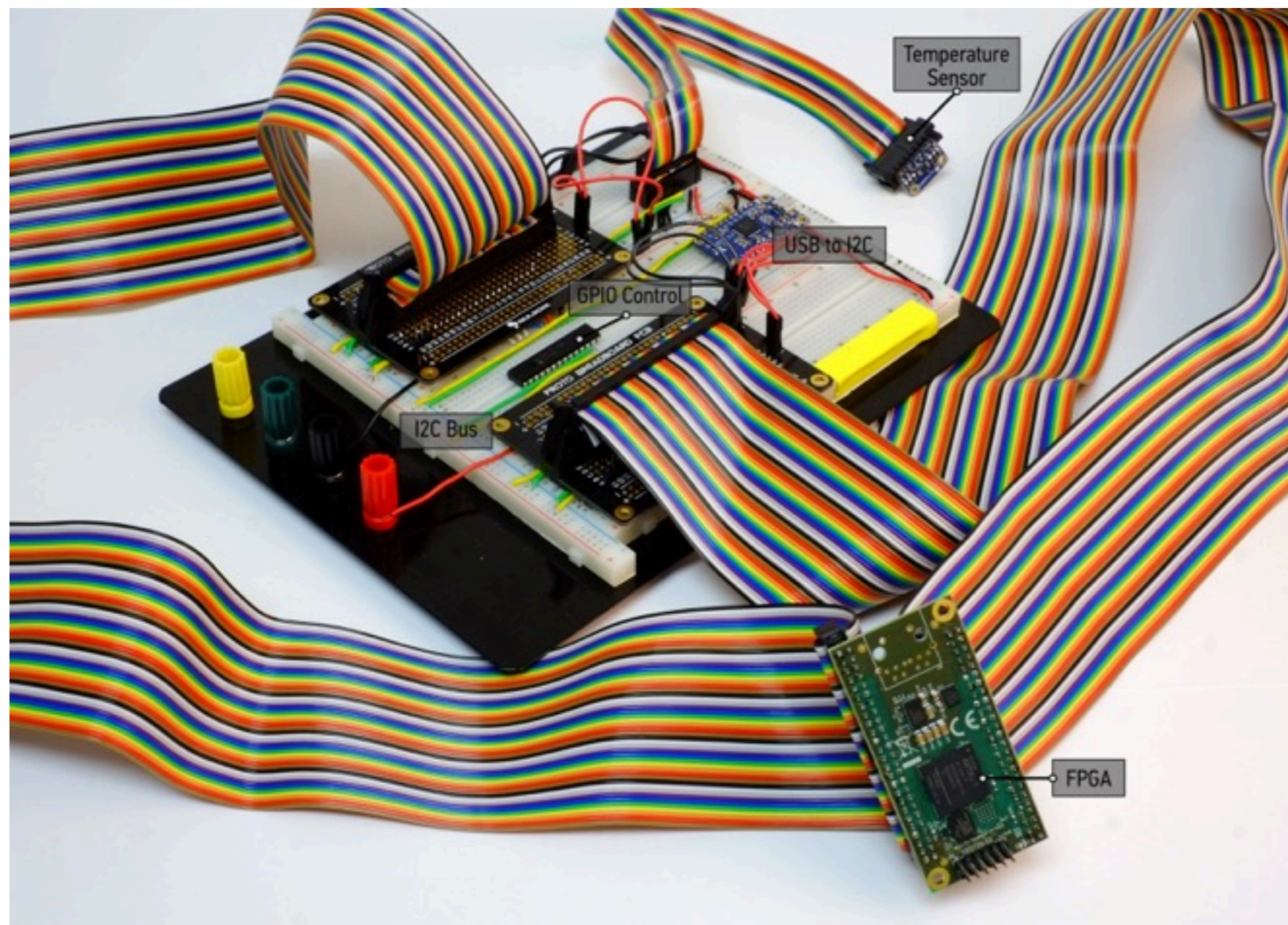
Xilinx Artix-7
FPGA

A Simplified 4 Inverter Ring Example



VP OF TEMPERATURE PROTOTYPE

EXPERIMENTAL RESULTS CONFIRMED PROOF-OF-PRINCIPLE



S. Philippe, M. Kütt, M. McKeown, U. Rührmair and A. Glaser, "The Application of Virtual Proofs of Reality to Nuclear Safeguards and Arms Control Verifications,"
Proceedings of the 57th Institute of Nuclear Materials Management Annual Meeting, 24-28 July 2016, Atlanta, Georgia.



CONSORTIUM *for* VERIFICATION TECHNOLOGY



Example 2



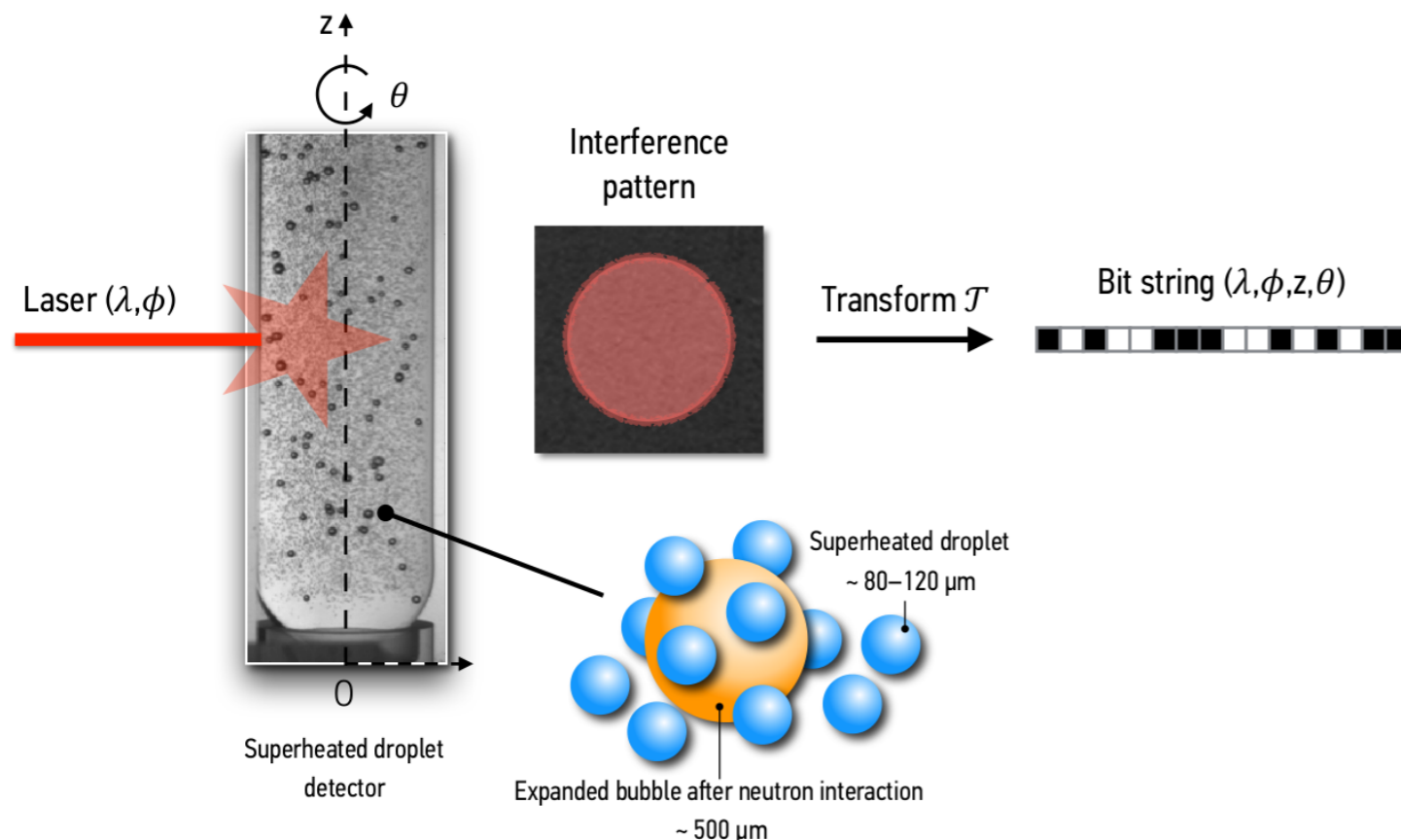
Example 2

A Virtual Proof of Neutron Non-Irradiation



VP OF NEUTRON NON-IRRADIATION

PROVING AN OBJECT HAS NOT BEEN EXPOSED TO NEUTRON



S. Philippe et al. INMM 2016.

- **Set-up Phase (Verifier):**
 - Preload detector
 - Create CRP-list
 - Transfer detector to Prover
- **Proof Phase:**
 - Prover claim detector hasn't been exposed to neutrons
 - Verifier send challenge (z, θ)
 - Prover shine laser at (z, θ) and send response to Verifier
 - If response sent = expected response from CRP-list, Verifier accept the proof

What Are Potential Applications for Virtual Proofs?



SOME RELEVANT AND POTENTIAL APPLICATIONS



CHALLENGE INSPECTIONS FROM A DISTANCE

Remote and trusted physical measurements (potentially constant monitoring).



CHAIN OF CUSTODY AND CONTINUITY OF KNOWLEDGE

Have treaty accountable items stored in a room been displaced? (freeze scenario)



PERIMETER CONTROL

Have radiation sources or plutonium been taken out of a room/building? (dismantlement)



DATA COMMITMENT

Allowing the Host to review the data first (facilitating imaging protocols)



BEYOND ARMS CONTROL

TRUSTED SENSOR NETWORKS AND IOT



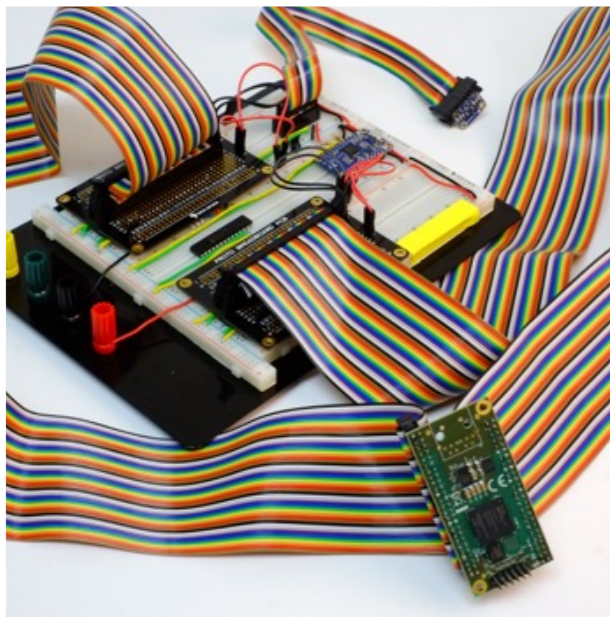
TAKE AWAY

ACQUIRING DATA IN PLACES WHERE WE HAVE NO ACCESS



GENERATING CREDIBLE INFORMATION

On-site inspections are a key mechanism for nuclear verification. But they are often hard to negotiate. Setting-up remote verification is an alternative but is limited by the ability to insure that data are trustworthy.



ENABLING TRANSPARENCY WITHOUT INTRUSIVENESS

Virtual Proofs of Reality offer a way to prove physical statements remotely without using classical tamper-resistant hardware and cryptographic keys. They have potentially important applications in nuclear verification.





MORE

nuclearfutures.princeton.edu/projects/

sebastienphilippe.org

ACKNOWLEDGEMENTS

U. Rührmair, A. Glaser, B. Barak,
M. Kütt & M. McKeown



CONSORTIUM *for* VERIFICATION TECHNOLOGY

