PUFs Breakout Session

Challenges and Opportunities of Physically Unclonable Functions Research

Moderator: Jakub Szefer
(Yale University)

10:30 am -12:00 pm
Tuesday, Jan. 10, 2017

SaTC PI Meeting ‘17

Session Logistics

- **PUFs breakout session info**
  - Room: Mt. Vernon - 2nd level/Capacity: 40
  - Time: 10:30am to 12:00pm

- **Goal: discuss PUFs research**
  - There will be no more presentation (after these intro slides)
  - Discuss and have fun talking about PUFs research

- **Need a scribe for the session**
  - No need to record every comment, but there should be some record we can combine with other session commentary as a general readout after the event. There will not be a live readout of the sessions at the PI meeting, so try to provide enough context for somebody to understand the substance of the discussion after the fact.

Topics for the Session

A **Physically Unclonable Function** (PUF) is a unique and stable physical characteristic of a piece of hardware, which emerges due to variations in the fabrication processes. PUFs have become an important and promising hardware primitive for fingerprinting, authenticating, or storing cryptographic keys in computing devices.

PUF research topics include: **design of devices and circuits** to be used for PUFs, **protocols** that leverage PUFs, error correction and **fuzzy extractors** used in the protocols, and **applications** (software) that use PUFs. Also, **modeling and attacks** on PUFs.

Background

- Ideas related to PUFs first came about in 1980s, hardware security community has explored PUFs in detail since 2000s.

- PUFs are not only of academic interest, as companies since 2010s have begun to include PUF instances in their products. For example, SRAM PUFs in Altera FPGAs (now part of Intel).

- This is an active academic research field, but also there is industry interest and actual applications. In about 30 years, initial ideas have turned into actual products.

Importance

PUFs can be used in a variety of scenarios:

- hardware identification
- anti-counterfeiting
- tracking computer hardware recycling
- generating cryptographic keys from the PUFs
- and more…

Advantages of using PUFs:

- cannot be easily cloned, even for the original manufacturer
- cannot predict the PUF before it is manufactured
- a PUF is a unique fingerprint for a device

Challenge Questions pt. 1

What’s next for PUFs?

- How can we advance research on devices for use with PUFs further?

- Have we reached stage where new research focuses only on showing X is a PUF, where X is your favorite device or material not used for a PUF before?

- How to promote adoption / further evaluation of novel PUF devices and circuits?

Challenge Questions pt. 2

How to evaluate PUFs?

- How can we promote researchers to make PUF measurements available so others can reproduce the work?
- How can existing data be used to try to attack the different PUF constructions (in order to find out problems with PUFs early)?
- Should we develop standard platforms for PUFs research (c.f. development platforms for power analysis and side-channels)?

Challenge Questions pt. 3

Extrinsic vs. Intrinsic PUFs?

- Should focus shift more to extrinsic PUFs and new devices or intrinsic PUFs that can be found in commodity devices?

- Do intrinsic or extrinsic PUFs have better future and possibility of adoption?

- What is best approach to expand PUF adoption, promote new PUFs for industry adoption, or find PUF instances in existing hardware?

Challenge Questions pt. 4

Research further up the stack?

- Most PUF research is on devices and PUF design, less on PUF protocols, and almost none on applications (software that uses PUFs). Is that the right balance?
- Should focus switch to more protocols and applications?
- What are the new protocols and applications?

Challenge Questions pt. 5

Exploring PUF-based protocols?

- Protocols for using PUFs are not very well developed, and almost none are verified or checked. How to show the protocols are correct?

- Can they be verified?

PUFs Breakout Session – Thank You!

Physically Unclonable Functions Research

Moderator: Jakub Szefer
(Yale University)

10:30 am -12:00 pm
Tuesday, Jan. 10, 2017

SaTC PI Meeting ‘17