Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions

Rafail Ostrovsky

UCLA (USA)

Alessandra Scafuro

Università di Salerno (ITALY)

Ivan Visconti

Università di Salerno (ITALY)

Akshay Wadia

UCLA (USA)

This presentation is not eligible for Best Presentation Award

UC Security [Can01]

Impossible when relying on computational assumptions only.

Achieved under various relaxed notions:

- ○ relaxed security
  (CRS [CLOS02], angels [PS04], super-polynomial time simulation [BS05])
- ○ relaxed concurrency
  (timing [KLP05], bounded concurrency [Lin03,PR03,Pas04])
- ○ physical assumptions
  (tamper-proof hardware [Kat07,CGS08,MS08,GKR08,GIS+10,DKMQ11])

This presentation is not eligible for Best Presentation Award

Physically Uncloneable Functions (PUFs) [PAP01,PRTG02]

A physical process generates a physical object that behaves similarly to a random function.

Generating two correlated objects is considered to be unfeasible.

This presentation is not eligible for Best Presentation Award

PUFs in Protocols

comparison with Random Oracles:

- random oracles are always publicly accessible
  - ➢ PUFs can be queried only when physically available
- random oracles can be programmed/simulated
  - ➢ not clear that the same can be done with PUFs
- random oracles are honest/trusted
  - ➢ should we trust PUFs produced by adversaries ?

This presentation is not eligible for Best Presentation Award

PUFs in Protocols

comparison with Tamper-Proof Hardware Tokens:

- Tokens are programmable/simulatable
  - PUFs are unpredictable only
- Tokens are constructed to behave as black boxes
  - PUFs are not necessarily black boxes
- Tokens are cloneable
  - PUFs are uncloneable
- Tokens can be stateful
  - PUFs are stateless

This presentation is not eligible for Best Presentation Award

UC Security with PUFs

C., Brzuska, M. Fischlin, H. Schröder, S. Katzenbeisser:
Physically Uncloneable Functions in the Universal
Composition Framework, CRYPTO 2011 ([BFSK11])

- minimalist model (uncloneability and unpredictability)
- PUFS are non-simulatable
- Unconditional UC Secure Computation

- only honest PUFs
- only honest access to PUFs

This presentation is not eligible for Best Presentation Award

UC Security with PUFs

BFSK11: honest generation of PUFs only ☹

○ is it safe to assume that a real-world adversary can not be able to produce a physical object that looks like a PUF but that internally includes a malicious behavior ?

- ➢ probably no… ☹

This presentation is not eligible for Best Presentation Award

UC Security with MALICIOUS PUFs

R. Ostrovsky, A. Scafuro, I. Visconti, A. Wadia
Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions,
http://eprint.iacr.org/2012/143

○ we give a new formulation of UC security where an adversary is allowed to have her own malicious PUF generation procedure

○ we show that UC Security is possible in our new formulation by relying on computational assumptions (in presence of PUFs)

This presentation is not eligible for Best Presentation Award

UC Security with Malicious Queries to PUFs

[BFSK11]: honest access to PUFs only

○ is it safe to assume that an adversary is not able to query a honest PUF using a different physical process ?

➢ perhaps no…

○ consequence:

➢ with PUFs, assuming that a simulator can see adversary's queries gives the same controversial flavour of non-standard non-black-box assumptions as the knowledge of exponent assumption (KEA)

➢ with UC security this is even more controversial since the simulator does not know the code of the environment

This presentation is not eligible for Best Presentation Award

UC Security with Malicious Queries to PUFs

R. Ostrovsky, A. Scafuro, I. Visconti, A. Wadia
Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions
http://eprint.iacr.org/2012/143

surprisingly we show that we can achieve UC security in presence of malicious queries to PUFs…. 😊

unconditionally! (same claim of [BFSK11] but modelling a stronger adversary!)

😊

This presentation is not eligible for Best Presentation Award

UC Security with Malicious Queries to PUFs

THANKS A LOT FOR YOUR PATIENCE !!!!!

This presentation is not eligible for Best Presentation Award