Fraunhofer
AISEC

Fraunhofer Institute for Applied
and Integrated Security AISEC

Seminar Verifiable Computation

Fraunhofer AISEC, Department Secure Operating Systems

Why Verifiable Computation?

Introduction

- Nowadays, Computation is heavily offloaded to other machines
  - Cloud computing, edge computing, …
- Machines are not controlled by the user!
  - Integrity of results cannot be guaranteed
- Possible Solutions:
  - Redundant Computation (e.g. SETI@home)
  - Verified Hard- and Software, Attestation, Trusted Root: TPM, Confidential Computing
- Verifiable Computation aims to remove the trust anchor
- Instead: generate a cryptographic proof of correctness during computation
- → Check this proof against the solution without (expensive) recomputing

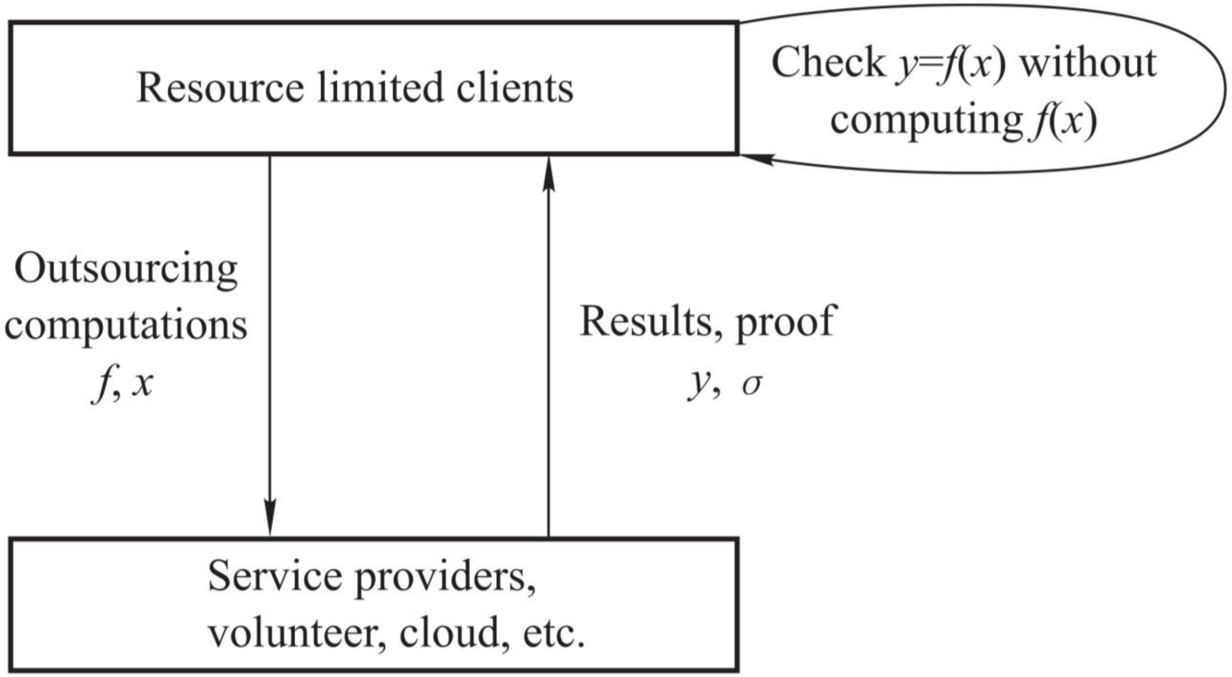
Resource limited clients
Check $y=f(x)$ without computing $f(x)$
Outsourcing computations
f, x
Results, proof
y, σ
Service providers, volunteer, cloud, etc.

Fig. 1: General Verifiable Computation Framework [Ahmad et al, 2018]

Seminar Topics

- Classes of Verifiable Computation Algorithms [Ahmad et al, 2018]
  - Interactive Proofs
    - Muggles
  - Zero-knowledge Proofs/Arguments
    - zkSNARKs
    - zkSTARKs
    - Bulletproofs
  - Probabilistically Checkable Proofs
  - Computationally Sound Proofs

- Applications include:
  - Verifiable Databases
  - Verifiable State Machines
  - Secure Cloud Control
  - Zero-knowledge Middleboxes
  - Blockchain?
  - ...

- Concrete topic and scope for each paper will be assigned based on the course occupancy and students' preferences

Scope of Papers

- Theoretical fundamentals
  - Mathematical theory of the considered method
  - Complexity
  - Assumptions about environment and setup
  - Security guarantees
  - Limitations

- Beyond their theoretical fundamentals, each considered method should be evaluated with respect to:
  - Physical requirements (i.e. CPU and memory consumption)
  - Real-world applicability (i.e. to which problems can this be applied?)
  - Existing Frameworks (i.e. do open-source implementations exist and are they usable/maintained?)
    - Are they limited to specific programming languages?
  - Existing Applications (i.e. is this actually used in the wild and what for?)

At a glance

Key Facts & Figures

- This course includes math and formal methods. You will most likely not be programming.
- Kick-Off: 10.08. 14:00 – 18:00; physical attendance is mandatory.
- Outline submission on 06.09.2023 23:59 Anywhere on Earth (= 07.09.2023 13:59 Munich Time)[1], 4 weeks after kickoff
- Paper submission on 15.11.2023 23:59 Anywhere on Earth (= 16.11.2023 12:59 Munich Time)[2], 10 weeks after outline
- Presentation slots:
  - Wednesday, 29.11.2023 14:00 – 17:00 CET
  - Thursday, 30.11.2023 14:00 – 17:00 CET
  - Friday, 01.12.2023 14:00 – 17:00 CET
  - Location TBD, but most likely at Fraunhofer AISEC
  - Physical attendance is mandatory.
- This seminar allows up to 9 students maximum and needs at least 3 students to take place.
- Requirements: IN0015, MA0901, IN0018, IN0042*
- Always communicate with course organizers through vcseminar@aisec.fraunhofer.de

[1]: https://www.timeanddate.com/worldclock/converter.html?iso=20230907T115900&p1=tz_aoe&p2=168

[2]: https://www.timeanddate.com/worldclock/converter.html?iso=20231115T115900&p1=tz_aoe&p2=168

*: Optional, but strongly encouraged

At a glance

Key Facts & Figures (con't)

- Group assignment (2-3 students)
- Improving scientific writing skills in Tex (15-20 pages, ACM template)[1]
- Presenting a scientific topic (in German/English):
  - 30 minutes (per student) + 15 minutes discussion.
- Enhancing theoretical and practical security skills

- Grading:
- Scientific paper: 50% (Content, Style, Effort, Grasp)
- Presentation: 40% (Content, Lecture Style, Understandability)
- Active participation/discussion: 10%

[1]: Will be provided to you at the kickoff meeting.

Fraunhofer
AISEC

Fraunhofer Institute for Applied
and Integrated Security AISEC

Contact

Katharina Bogad, Barbora Hrdá, Johannes Wiesböck
Secure Operating Systems
Tel. +49 89 3229986-{1020,167,1046}
vcseminar@aisec.fraunhofer.de

Fraunhofer AISEC
Lichtenbergstr. 11
85748 Garching near Munich
Germany
www.aisec.fraunhofer.de