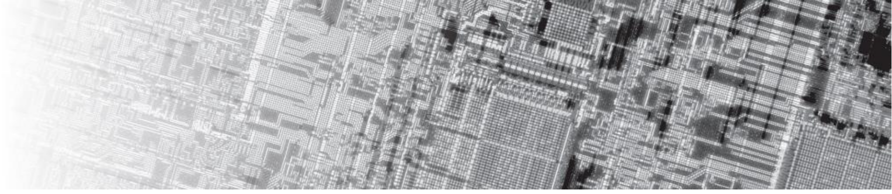
RESCUE
European Training Network



Secondment report

Name: ESR2.4 Xinhui Lai
IRP title: **Functional and non-functional verification and debug methods for complex nanoelectronic systems**
From: TUT
To: IID
Period: May 05 – June 02,2019

Activities during the secondment

- **Scope and objectives:**
  - Security aspect verification. The object of this cooperation is to research timing side channel attack on SRAM PUF.
- **Activities:**
  - SRAM PUF research topic discussions with IID
  - SRAM PUF and error correction code study
  - Regular skype meetings for updating and discussions
  - Attending IID internal presentation
- **Main results achieved:**
  - Understand SRAM PUF and error correction code
  - Identify the timing side channel vulnerable component of SRAM PUF
  - Make the research plan to study timing and power side channel attack of error correction code decoder
- **Next steps:** Research on timing and power side channel attack vulnerability analysis of error correction code decoder.
- **Optional request for support or a technology/tool available at host:** No

Self-evaluation

Overall score: 4.5
I consider this secondment successful, with regards to the research objectives achieved, skills developed, supervision quality, diversity of the resources. (Agree = 5 … Disagree = 1)
Optional comments:
No
Date of the report approval by the supervisor: 18.11.2019

The RESCUE ETN project has received funding from the European Union’s Horizon 2020 Programme under the Marie Skłodowska-Curie actions for research, technological development and demonstration, under grant n. 722325.