PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 36th cycle

Research Area n. 1 - Computer Science and Engineering

Research Field: HARDWARE IMPLEMENTATION OF POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS FOR THE IOT

<table>
<thead>
<tr>
<th>Monthly net income of PhD scholarship (max 36 months)</th>
</tr>
</thead>
<tbody>
<tr>
<td>€ 1300.0</td>
</tr>
</tbody>
</table>

In case of a change of the welfare rates during the three-year period, the amount could be modified.

Context of the research activity

The recent developments in quantum-computing are posing contemporary public-key cryptographic solutions, that are based on the intractability of either the discrete logarithm problem or the integer factorization problem, under a serious threat. As a consequence, research communities ranging from mathematical to engineering ones, as well as standardization agencies have started dealing with the problem of designing security systems that could resist the overcome of quantum computers, so called post-quantum or quantum-safe systems. STMicroelectronics will sponsor a PhD grant to foster research on how post-quantum cryptographic schemes can be effectively and efficiently implemented with a special focus on dedicated hardware accelerators or fully-customized hardware implementations. The outcomes of this research are expected to improve significantly the performance figures (i.e., latency, throughput, energy) for the entire range of Internet-of-Things (IoT) platforms, ranging from microcontrollers and smart cards to small single board computers. Tackling the design of specialized hardware to provide secure and energy efficient cryptographic primitives allows also to embed countermeasures against side channel attacks which will be designed taking into account the trade-offs between the overheads and the additional security margin.
Methods and techniques that will be developed and used to carry out the research

The research will rely and improve the candidate’s knowledge and capability to use the building blocks needed to design and implement public-key cryptographic primitives together with the ability to cope with concrete engineering challenges arising from the design and realization of side channel secured implementations.

Educational objectives

The PhD candidate will develop a strong background in modern cryptography, hardware design and embedded systems, together with strong engineering skills thanks to the strict collaboration with our industrial partners. The latter will entail developing a concrete and valuable perception of the engineering constraints which are met in real world industry grade devices.

Job opportunities

The PhD candidate will address problems with a broad applicability in the field of security technologies. A PhD graduate with such a background can be very valuable in STMicroelectronics as well as many other large companies / SMEs.

Composition of the research group

- 0 Full Professors
- 3 Associated Professors
- 0 Assistant Professors
- 3 PhD Students

Name of the research directors

Gerardo Pelosi

Contacts

gerardo.pelosi@polimi.it
02 2399 3476
http://home.deib.polimi.it/pelosi/

| Additional support - Financial aid per PhD student per year (gross amount) |
|-------------------------------------------------|-----------------|-----------------|
| Housing - Foreign Students                      | 1st year | 2nd year | 3rd year |
|                                                 | 1500.0 € per student | 1000.0 € per student | 1000.0 € per student |
| Housing - Out-of-town residents (more than 80Km out of Milano) | -- |

max number of financial aid available: 4, given in order of merit ..
LIST OF UNIVERSITIES, COMPANIES, AGENCIES AND/OR NATIONAL OR INTERNATIONAL INSTITUTIONS THAT ARE COOPERATING IN THE RESEARCH: Politecnico di Milano; ST Microelectronics, SRA

The PhD will be co-supervised by the Security team in the SRA (System Research and Applications) organization at STMicroelectronics. The Security team features 16 senior researchers, 4 in Agrate and 12 in Rousset, and a few MSs students that are doing their stage in STMicroelectronics. PhD candidate will be asked to contribute to the MSs students’ supervision, and to do regular visits in STMicroelectronics.

INCREASE IN THE SCHOLARSHIP FOR STAYS ABROAD: Euro 566.36 per month, for up to 6 months

EDUCATIONAL ACTIVITIES (purchase of study books and material, including computers, funding for participation in courses, summer schools, workshops and conferences): financial aid per PhD student per year
2nd year: euros per student (1534)
3rd year: euros per student (1534)

TEACHING ASSISTANSHIP: (availability of funding in recognition of supporting teaching activities by the PhD student)
There are various forms of financial aid for activities of support to the teaching practice. The PhD student is encouraged to take part in these activities, within the limits allowed by the regulations.

COMPUTER AVAILABILITY:
1st year: individual use
2nd year: individual use
3rd year: individual use

DESK AVAILABILITY:
1st year: individual use
2nd year: individual use
3rd year: individual use