

## 1 Research Position

### Light-weight crypto primitives, suitable for body sensor networks

CTIT

The Centre for Telematics and Information Technology (CTIT) is a multidisciplinary research institute of the University of Twente, Enschede, The Netherlands. CTIT coordinates the research activities in all the areas relevant to the development, the introduction and the usage of information technology systems. <http://www.ctit.utwente.nl/>

### Project Description

There is a re-emerging demand for low-end devices driven by needs for pervasive applications like wireless sensor networks (WSN) and body sensor networks (BSN). Security in pervasive applications, however, has been a major concern for their widespread acceptance. In particular, the security requirements for body sensor networks turn out to be significantly different from those of wireless sensor networks. For example, in the deployment of a BSN we are more interested in exceptions (high blood pressure) than the rule (the average temperature of a potato field). Another important issue is that the data in a BSN is privacy sensitive, because it applies to a person and not to a plant, animal or inanimate object.

### Research

To address the ensuing stringent security requirements in a BSN, we have to be prepared to expend more of the precious resources of a sensor node to security than in a WSN.

To compensate for this, we note that a BSN is typically smaller, and exists in a more benign environment than a WSN. The main challenge in BSN is to design secure cryptographic primitives that will not consume extensive resources.

*The research topic* of the PhD student will be **to design secure symmetric cryptographic primitives and/or secure protocols (suitable for such primitives) which use limited resources**. Design of crypto algorithms for such constrained environments adds additional not security related but equally important requirements to the design process. Examples are gate equivalence of the hardware implementation and its power consumption or agility, throughput, etc. In order to achieve them often difficult tradeoffs have to be made as well as the appropriate security level has to be chosen for the particular application. Because the security level is usually optimized up to the edge the design of such symmetric crypto algorithms and protocols is a very challenging task.

### Selected References

- [1] G. Z. Yang (Ed). Body Sensor Network. Springer London, ISBN: 1-84628-272-1, 2003.
- [2] C. Paar, A. Poschmann, and M. Robshaw. New Designs in Lightweight Symmetric Encryption. In P. Kitsos, Y. Zhang (Eds.) RFID Security: Techniques, Protocols and System-on-Chip Design. Springer, pp. 349-371, 2008.
- [3] Zheng Gong, Pieter Hartel, Svetla Nikova, Bo Zhu and Weidong Qiu, Towards Secure and Practical MACs for Body Sensor Networks, Technical Report CTIT, University of Twente.
- [4] S. Indestege, E. Andreeva, C. De Cannière, O. Dunkelman, E. Käsper, S. Nikova, B. Preneel, and E. Tischhauser, "The Lane Hash Function -- Extended Abstract," COSIC internal report, 14 pages, 2008.

### What we ask and what we offer

You have completed a university education or are about to graduate in an area that is relevant to our research, i.e. computer science, electrical engineering, or mathematics. You like working in a team and have knowledge of one or more of the following topics: data bases, networking, and security. Your main task will be to do research, but you will be given the

opportunity to acquire some teaching experience. As PhD student you will be appointed for a period of four years, at the end of which you must have completed a PhD thesis. During this period you have the opportunity to broaden your knowledge by joining international exchange programs, to participate in national and international conferences and workshops, and to visit other research institutes and universities worldwide. The PhD students will be appointed at CTIT. The monthly salary of a PhD student ranges from EURO 1956,- gross in the first year to EURO 2502,- gross in the fourth year.

**Information and application**

More information may be obtained from Dr. Svetla Nikova ([s.i.nikova@utwente.nl](mailto:s.i.nikova@utwente.nl)) or Prof. Pieter Hartel ([pieter.hartel@utwente.nl](mailto:pieter.hartel@utwente.nl)). You are invited to send your application together with curriculum vitae, marks transcripts and the names and addresses of two referees by email to [jobs@ctit.utwente.nl](mailto:jobs@ctit.utwente.nl).