Abstract

Technological advancements in the semiconductor industry over the last few decades made the mass production of very small-scale computing devices possible. Thanks to the compactness and mobility of these devices, they can be deployed “pervasively”, in other words, everywhere and anywhere – such as in smart homes, logistics, e-commerce, and medical technology. Embedding the small-scale devices into everyday objects pervasively also indicates the realization of the foreseen “ubiquitous computing” concept. However, ubiquitous computing and the mass deployment of the pervasive devices in turn brought some concerns – especially, security and privacy.

Many people criticize the security and privacy management in the ubiquitous context. It is even believed that an inadequate level of security may be the greatest barrier to the long-term success of ubiquitous computing. For ubiquitous computing, the adversary model and the security level is not the same as in traditional applications due to limited resources in pervasive devices – area, power, and energy are actually harsh constraints for such devices. Unfortunately, the existing cryptographic solutions are generally quite heavy for these ubiquitous applications. In order to address the security problem of the resource-constrained devices, “lightweight cryptography” has been defined over a decade ago and many different lightweight cryptographic primitives have already been proposed. The published work so far mostly deals with hardware cost reduction. However, this is not the only important metric for such devices. Depending on the application, resource-constrained devices may need lightweight ciphers to be executed in one clock cycle, which still achieve a certain security level and a small footprint. Furthermore, as most of the pervasive computing applications are implemented in software on embedded microcontrollers, there is also a need for lightweight ciphers that result in efficient code size and execution time.

In this thesis, we understand lightweight cryptography also as “resource-efficient cryptography” and we aim to provide new “resource-efficient” solutions for resource-constrained devices, which address the mentioned gaps in lightweight cryptography. We start with initial investigations on existing lightweight primitives, where we present efficient implementations on different platforms, their applications, and comparisons. In the light of our initial investigations, we first propose a new low-latency and low-area lightweight block cipher PRINCE. Following PRINCE, we change our direction to the software side – targeting the software implementations on microcontrollers. As a first step, we come up with a hardware/software co-design approach, the Non-linear/Linear Unit (NLU) Instruction Set Extension (ISE), which targets the 8-bit AVR instruction set of widely-used Atmel microcontrollers. After that, we extend our approach more on the primitive design side, where we define another new lightweight cipher, the “software-oriented” lightweight cipher PRIDE.

In addition to our contributions on efficient lightweight primitive implementations presented in the first part of this thesis, the two novel lightweight block cipher designs achieve the targets and present the best academic results published so far. In the ISE design, our good results
encourage further block cipher extensions on different microcontrollers in order to get a better code size and execution time. However, it is of course not easy to overcome all the gaps in lightweight cryptography in one work. Therefore, other designs and solutions addressing different metrics still remain as an open research problem left for future works.

**Keywords.**

Lightweight cryptography, resource-efficient cryptography, design, ubiquitous computing, symmetric-key cryptography, block cipher, hash function, hardware implementation, software implementation, Application Specific Integrated Circuit (ASIC), Field Programmable Gate Array (FPGA), microcontroller, Atmel AVR, IT Security