**Design and Implementation of High-Quality Physical Unclonable Functions for Hardware-Oriented Cryptography**

**A. A. Ivaniuk 1**

**S. S. Zalivaka**

**L. Zhang**

**V. P. Klybik**

**Ch.-H. Chang**

## 1 Белорусский государственный университет информатики и радиоэлектроники

**Abstract:** Physical Unclonable Functions have emerged as effective primitives for varieties of security applications. With the advent of mobile computing, designing and implementing high-quality PUFs for resource-constrained platforms become a great challenge. This chapter presents an extensive review of the techniques proposed in the recent years for the design and implementation of high-quality and/or

alternative PUF instances with marginal overhead. With a preamble of the motivations, fundamentals, quality metrics and application scenarios of PUF, some existing approaches to improving the quality of PUFs are unfolded. Subsequently, some representative PUF designs for RFIDs and fingerprint extractions are illustrated. In addition, applications for true random number generation based on PUF instances are delineated. Finally, two emerging types of PUF implementations that can be used for more advanced protocols are presented. The practices summarized in this chapter aim to help the engineers and researchers in the hardware security community to design and implement PUFs that suit their applications and constraints.

**Keywords:** Keywords: trustable computing, physically unclonable functions, digital design.

**Internet link to the article**: <http://www.springer.com/la/>book/9783319149707