A Formal Definition and a New Security Mechanism of Physical Unclonable Functions

Rainer Plaga and Frank Koob

Federal Office for Information Security (BSI), D-53175 Bonn, Germany
{rainer.plaga,frank.koob}@bsi.bund.de

Abstract. The characteristic novelty of what is generally meant by a “physical unclonable function” (PUF) is precisely defined, in order to supply a firm basis for security evaluations and the proposal of new security mechanisms. A PUF is defined as a hardware device which implements a physical function with an output value that changes with its argument. A PUF can be clonable, but a secure PUF must be unclonable.

This proposed meaning of a PUF is cleanly delineated from the closely related concepts of “conventional unclonable function”, “physically obfuscated key”, “random-number generator”, “controlled PUF” and “strong PUF”. The structure of a systematic security evaluation of a PUF enabled by the proposed formal definition is outlined. Practically all current and novel physical (but not conventional) unclonable physical functions are PUFs by our definition. Thereby the proposed definition captures the existing intuition about what is a PUF and remains flexible enough to encompass further research.

In a second part we quantitatively characterize two classes of PUF security mechanisms, the standard one, based on a minimum secret read-out time, and a novel one, based on challenge-dependent erasure of stored information. The new mechanism is shown to allow in principle the construction of a “quantum-PUF”, that is absolutely secure while not requiring the storage of an exponentially large secret. The construction of a PUF that is mathematically and physically unclonable in principle does not contradict the laws of physics.

1 Introduction

1.1 Aims and Outline of This Work

“Physical unclonable functions” (PUFs) are electronic hardware devices that are hard to reproduce and can be uniquely identified [14,8]. They promise to enable qualitatively novel security mechanisms (see e.g. [2,9,10]) and have consequently become a “hot topic” in hardware security [5]. The present work asks the question “What characteristics exactly define the qualitative novelty of the PUF concept?”. We hope that a precise answer will aid the security evaluation of existing PUFs and help to develop new ideas for PUF security mechanisms. We searched for
1. a formal definition of the properties that are required from a hardware device to be called “PUF”, and a
2. a formal definition of the criteria that have to be fulfilled to consider a PUF “unclonable”.

The formal PUF definition should not suffer from weaknesses of previous definitions (see section 1.2), encompass at least the large majority of the existing PUF constructions, and be as flexible as possible, i.e. does not restrict further progress in PUF development (e.g. by demanding constructional details, like the amount of stored information). This aim is achieved in section 2.1. After formulating a simple definition of PUF-security (based on Armknecht et al.) in section 2.2, we delineate PUFs from some closely related security concepts (section 3) and outline the elements of a PUF-security evaluation (section 4).

In a second part of the paper we systematically analyse and classify PUF security mechanisms and calculate their quantitative security levels against attacks that attempt mathematical cloning (section 5). The aims of this section are to give a quantitative answer to Maes & Verbauwhede’s question whether mathematically-unclonable PUFs are possible in principle, and to apply and thereby illustrate the PUF-definitions of the first part of the paper. In section 6 we characterise the qualitative novelty of PUFs as a new primitive of physical cryptography and discuss the future use and development of PUFs.

1.2 Previous Work on the Definition of a PUF

There have already been several proposal for the first definition of required PUF properties. Gassend et al. who invented the term “PUF” (earlier work by Pappu was on the slightly different concept of a physical one-way function) demand that the function must be “easy to evaluate”, i.e. it must efficiently yield a response value “R” for a challenge argument “C”. and “hard to predict (characterize)”. The latter property means that an attacker who has obtained a polynomial number of C – R pairs (CRPs) but has no longer physical access to the PUF can only extract a negligible amount of information about the R for a random C. Rührmair et al. criticised this definition because the information content of finite physical objects is always polynomially bound, and therefore no PUF fulfilling this definition can exist. They propose an alternative formal definition in which the PUF must only be hard to predict for an attacker “who may execute any physical operation allowed by the current stage of technology”. Maes & Verbauwhede chose to exclude unpredictability from their “least common property subset” of PUFs, because they put into question whether it is possible in principle to construct a mathematically unclonable PUF. They demand that a PUF is “easy to evaluate” (property “evaluatable”) and that it is “reproducible”, meaning that a C always leads to the same R within a small error. Moreover they demand “physical unclonability” i.e. that it must be “hard” for an attacker to construct a device that reproduces the behaviour of the PUF. However, PUFs that are mathematically clonable are also physically clonable because the mathematical algorithm for PF can then be implemented.