Master Thesis

Chair for Theoretical Information Technology

RWTH AACHEN UNIVERSITY

Error Correction for Variable-Length PUF Quantization

Research Area

information theory, error correction code, hardware security

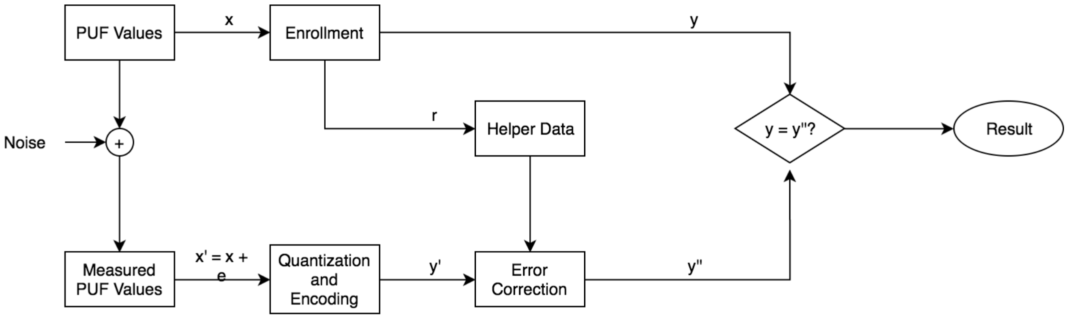
Keywords

Physical Unclonable Functions, variable-length codes, insertion/deletion error correction

Description

Physical Unclonable Functions (PUFs) are used for key storage in security applications. They extract the unique physical characteristics from a device to generate public helper data and a private key. To achieve both reliability and robustness in the presence of noise, the input values are quantized to remove noise to some extent. Furthermore we perform error correction to mitigate when a quantized value falls into adjacent intervals. There are two different approaches for choosing quantization intervals namely equiprobable quantization and equidistant quantization both using fixed-length coding. These two approaches have tradeoffs between bias and information leakage. In fixed-length coding, the bias is observed when one quantized symbol has a higher probability to occur than others. The information leakage, defined as the mutual information between the helper data and the key, evaluates how much knowledge of the key can be extracted by attackers.

To prevent information leakage and to eliminate the bias, this thesis introduces variable-length coding to equidistant quantization. Since the length of each codeword is different, the decoder needs to be able to correct insertion/deletion errors. The quantization and encoding process is assumed to have following characteristic: when a value interfered by noise is incorrectly quantized into another interval, the new quantized value should only have one bit inserted/deleted/flipped from its original value, and the decoder should be able to correct the errors to some extent, i.e, the bitstream y'' should be the same as the reference bit stream y when the noise e is small.



Goal

The goal of this thesis is to build a whole simulation system, which contains quantization, encoding and error correction parts that ensure the authentication process of PUFs to have both reliability and robustness. Different error correction theories on insertion/deletion/substitution codes may be explored if necessary. If time permits, software or hardware implementation may be added to the work package.