Double Error Cellular Automata-Based Error Correction with Skip-mode
Compact Syndrome Coding for Resilient PUF Design

ABSTRACT

Physical Unclonable Functions (PUFs) present an attractive security primitive due to their volatile key generation capability. Subject to environmental conditions, the PUF response, however, is prone to errors which may undermine the reliability of the system when left unaddressed. An error-correction scheme is typically used alongside the PUF circuit when used for cryptographic applications. In this paper, we propose the use of Cellular-Automata Error-Correcting Codes (CAECC) due to their simplicity and regularity. An efficient implementation of (15, 7, 5) CA-ECC encoder/decoder targeting a Xilinx Zynq-7000 device is demonstrated, and the design is validated on design compiler targeting 40nm TSMC technology. We also propose a skip-mode compact syndrome coding scheme for relaxed per-block BER. CAECC is tested in conjunction with the skip-mode scheme, and the approach is verified on ring oscillator PUF data. The skip-mode scheme is found to reduce the ring oscillator overhead up to 20% and enhance the entropy up to 23% compared to no-skip schemes.

Existing System:

conventional ECCs such as BCH codes whose irregularity and decoding structure complexity increase with the number of information bits. Before discussing the proposed schemes, it is useful to have an overview of the 4-bit burst error correction codes that have been proposed so far to protect memories. Most of those schemes are based on the use of a two dimensional product code or matrix code. In those codes, data bits are arranged in the format of a matrix and parity bits are added horizontally and vertically. Depending on the horizontal and vertical codes used, different error correction capabilities can be achieved.
Proposed System:

In this paper, we evaluate for the first time the CA-based ECC code in the context of a newly proposed skip-mode CSC scheme on RO PUF data obtained from. The skip-mode scheme is proposed to relax the per-Block bit error rate in the event of most probable adjacent RO rank flips. We also evaluate the design complexity of CAECC by simulating a CAECC encoder/decoder blocks. In conjunction with CAECC, skip-mode CSC is proposed to relax the number of per-block bit errors for the most probable adjacent rank flips. This helps enhance the correction capability and reduce stability ifth. Theoretical studies as well as grouping analysis based on RO-PUF data demonstrate enhanced entropy and reduced hardware overhead by up to 20% for the skip-mode CSC compared to no-skip mode.

Applications

1) Communications
2) Digital signal processing

Advantages

Area, delay and power reduced

System Configuration:

In the hardware part a normal computer where Xilinx ISE 14.3 software can be easily operated is required, i.e., with a minimum system configuration

HARDWARE REQUIREMENT

<table>
<thead>
<tr>
<th>Processor</th>
<th>Pentium –III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>1.1 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>1 GB (min)</td>
</tr>
<tr>
<td>Hard Disk</td>
<td>40 GB</td>
</tr>
</tbody>
</table>
Floppy Drive - 1.44 MB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

Software Requirements

- Front End : Modelsim 6.3 For Debugging And Xilinx 14.3 For Synthesis And Hard Ware Implementation

*This Software’s where Verilog Source Code Can Be Used For Design Implementation.