Abstract

A new chip ID generation method is presented that leverages the random and permanent characteristics of oxide breakdown. A 128b ID array is implemented in 65nm CMOS and two algorithms for stressing the oxides are presented, showing a near-ideal Hamming distance of 63.92 in silicon measurements and consistent IDs across voltage and temperature.

Introduction

Chip ID systems are used to enforce user licenses as well as in communication and security protocols. In these applications, it is desirable to generate IDs on-chip at the application point so IDs are guaranteed unknown until first used. This avoids the need for off-chip, pre-generated IDs that are programmed using fuses, a process that exposes IDs to human intervention and storage on computers that may be compromised.

A key requirement for chip ID generation is that the generated ID is unique to only that chip, and that the ID is time and environmentally invariant. The chances that two chip IDs have all, or many, bits the same is minimized by using a large bit width (e.g., 128bits/ID) and ensuring a high degree of randomness during generation. Previous methods rely on inherent threshold voltage (V\text{t}) mismatch between devices, which is detected by measuring either device current or inherent SRAM bitcell skew towards 0 or 1 mismatch between devices, which is detected by measuring either device current [1] or inherent SRAM bitcell skew towards 0 or 1 states [2]. However, V\text{t} mismatch can be very small between any particular transistor pair, making it difficult to repeatedly generate an identical ID for a given chip. Hence, previous approaches exhibit a small number of bit flips between successive ID readings (i.e., the IDs had a non-zero self Hamming distance), complicating the use and reliability of chip IDs.

This paper presents a new method called OxID that generates chip IDs using oxide breakdown. We leverage the fact that oxide breakdown is an inherently random effect [3] (one oxide may break long before another identical oxide under the same stress conditions) and is also both abrupt and permanent. Hence, it enables improved ID stability over time and environmental conditions. Once an oxide breaks down, its resistance changes from a nearly infinite value to the order of M\Omega or k\Omega [4], which has made it popular for one-time-programmable arrays [5,6]. Silicon measurements of 162 ID generators in this work demonstrate nearly ideal randomness of the generated IDs, maximizing their uniqueness. The proposed approach can also detect prior ID generation; if on first use the ID is non-zero, this indicates that the ID was previously generated through possible intrusion and may be compromised.

Proposed System and ID Generation Method

OxID consists of a memory array composed of 3-T memory cells that use a thin-oxide moscap as a fuse element (Figs. 1 and 2). The array has 16 rows by 8 columns, totaling 128 cells, each of which can be read through a bitline and sense amplifier. All oxides in the array are exposed to a stress voltage of 4.5V and identical stress duration. Due to limitations of stress isolation a few borderline oxides may break down as well. Hence, this process sacrifices a small Hamming distance degradation (measured at 2-3%) for higher read operation robustness across environmental conditions.

The 3-T bitcell (Fig. 3) consists of a thin-oxide SVT transistor driven by the wordline, a thick-oxide 2.5V I/O “blocking” transistor, and a thin-oxide SVT transistor with S/D tied as a moscap. This bitcell is similar to the 3-T cell in [4,7]. The thick-oxide transistor separates the thin-oxide wordline device from the high voltage of the moscap during stress. For unbroken oxides there is by design a small voltage that accumulates across the moscap due to its high leakage at high V\text{DD} (0.7V for V\text{DDH} of 4.5V). This protects oxides that have not been selected for stress. Cell currents are limited by the resistance of the minimum-sized thick-oxide transistor and word-access transistor. During cell read, V\text{DDH} is shorted to V\text{DD}. For experimentation, the 128 oxides can be stressed all at once or by row, column, or cell.

Measurement Results

OxID was implemented in a standard 65nm CMOS technology. For experimentation, the gate voltage for the blocking transistor (VBT) and the sense amplifier reference voltage were brought in from off-chip, but can also be generated on-chip. We applied the global stress algorithm described above at room temperature to 162 arrays and the canary-based algorithm to 144 arrays. Two perfectly random IDs should, on average, have a Hamming distance of exactly half the total number of bits in the ID. Comparing all pairs of ID bit sequences (13041 and 10296 pairs, respectively), the average Hamming distance for the global algorithm is 63.92, close to the ideal value of 64 (Fig 4). The average Hamming distance for the canary algorithm is 61.79, implying a trade-off in randomness and ID set size (Fig 5). The read power is 0.34 pJ per bit (Table 1). The self-Hamming distance upon repeated reading of the ID in different environmental conditions was tested for 14 arrays. Results show 0 self-Hamming distance for up to 100mV supply voltage deviation from 1.1V nominal and across temperature from 0°C to 85°C. Figs. 7 and 8 show the self-Hamming distance as a function of voltage and sense amplifier read margin across temperature. Fig. 9 shows the generated bits for each cell location, averaged across all arrays, with no obvious spatial artifacts. The spatial distribution of the breakdown time of each oxide in a typical array is shown in Fig 6. Table 1 provides a comparison of OxID to related prior work [1,2], showing improved energy, stability, and density. Fig. 10 shows the number of stress intervals across all arrays. Fig. 11 shows the chip microphotograph and chip statistics are included in Table 2.

Acknowledgements

We thank STMicroelectronics for test chip fabrication support.
Table 1: Comparison with previous work

<table>
<thead>
<tr>
<th>Work</th>
<th>Throughput (Bps)</th>
<th>Energy per bit (pJ/bit)</th>
<th>Average Unstable Bit</th>
<th>ID Length</th>
<th>Technology (nm)</th>
<th>Area (um²)</th>
<th>Area Scaled to 65nm (um²)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>3.75k</td>
<td>8330</td>
<td>N/A</td>
<td>112</td>
<td>350</td>
<td>23,496</td>
<td>939.84</td>
</tr>
<tr>
<td>[2]</td>
<td>125k</td>
<td>0.93</td>
<td>3.9</td>
<td>128</td>
<td>130</td>
<td>15,288</td>
<td>3822</td>
</tr>
<tr>
<td>This work</td>
<td>625M</td>
<td>0.34</td>
<td>0</td>
<td>128</td>
<td>65</td>
<td>1242</td>
<td>1242</td>
</tr>
</tbody>
</table>

Table 2: Chip statistics

<table>
<thead>
<tr>
<th>Global Algorithm</th>
<th>VDD</th>
<th>Bit Length</th>
<th>Throughput (Bps)</th>
<th>Average Hamming Distance (162 arrays)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.1 V</td>
<td>128</td>
<td>625 M</td>
<td>63.92</td>
</tr>
</tbody>
</table>

References