Mitigating Row Hammer Attacks Based on Dummy Cells in DRAM

Andres Amaya, Hector Gomez and Elkim Roa
Integrated Systems Research Group, Onchip - Universidad Industrial de Santander, UIS
Bucaramanga, Santander, Colombia
{hector.gomez,andres.amaya1}@correo.uis.edu.co, efroa@uis.edu.co

***Abstract*—This paper presents an alternative to prevent data corruption in DRAM memories due to Row Hammer attacks. The proposal is based on the usage of dummy cells connected to each row as attacks indicator. These special cells are characterized for having a higher sensitivity to coupling noise. The strategy was validated by simulations on a 65nm CMOS 64x64 memory array, including process variations for coupling and interconnections. Results keep congruence with a memory dedicated, state-of-art, process of 28nm. The main characteristics of this suggested solution are its low-complexity and low-hardware overhead.**

I. Introduction

Fault modeling and testing are very time-consuming tasks in DRAM design. Reason why companies prize their DRAM products depending on the length of the applied test. This kind of analysis is based on different algorithms aimed for different types of faults such as stuck-at, transition, coupling and address decoding faults. In addition, coupling faults are becoming important in new technologies because of the continued shrinking of devices. Given that the increased density has a negative impact in memory performance and reliability because a small cell has a reduced noise margin due to its low capacity to hold charge. Also, the proximity between cells increases the electromagnetic coupling effects [1], [2].

Coupling noise in adjacent rows increases the leakage current of memory cells when a specific memory address is repeatedly opened (or activated), read and closed. The phenomenon of increasing leakage current in cells of adjacent rows due to the consecutive opening of a given row is called row hammering. Recently, many works have shown how row hammering causes bit flips or data corruption in modern DRAM chips [1]–[3]. Furthermore, it has been proved that row hammering can be used to achieve privilege escalation. For instance, a modified-video reproduction can be used to trigger this attack with the possibility to take control of a computer [4] as illustrated the Fig. 1.

Some mitigation strategies have been reported in the literature. In one hand, software strategies compound solutions such as increasing refresh rate or reducing the time to activate error correction algorithms. However, these software strategies can induce a large performance overhead, reducing their effectiveness in practical applications. On the other hand, hardware strategies are also found in some works and divided in two approaches: counter based and probabilistic row refresh. The first one consists in counting to activate a control signal including high performance overhead [1]. The second one avoids the need of storage information of the counters by reducing the needed hardware due to the probabilistic operation [2].

II. Dummy Cell Based Mitigating Strategy

The proposed strategy consists in connecting a dummy cell to the wordline of the victim row, as indicated in Fig. 2. The additional cell is similar to a standard memory cell but more susceptible to leakage. This characteristic can be achieved by implementing a transistor of twice its size regarding its nominal value, and a capacitor of a half its capacity. A wider transistor has a larger leakage current that, combined with the reduced storage capacity, results in a cell with a decreased retention time.

A cell with this particular attribute can be used as an indicator of a possible attack as follows: first, the dummy cell of a victim wordline must be pre-charged to logic level one (1) during the refresh phase. Then, if a malicious memory access is carried-out, the dummy cell will experiment a larger leakage current than a standard cell, thus its capacitor will be discharged with a increased rate. Therefore, the information stored in the dummy cell will be corrupted before the data of standard cells. Therefore, the memory controller might sense dummy cells data triggering a refresh of the respective victim row or near ones when it detects a zero logic preventing data-corruption.

The Fig. 3 shows an alternative to include dummy cells in a DRAM memory array. The dummy cells should share the respective bitline reducing complexity in control algorithm as memory controller only have to monitor one column address. Nonetheless, dummy cells can be placed in a sparse way across the array, in order to avoid that an attacker can easily identify their position. In addition, dummy cells can be implemented using combinations of 2X, 4X or larger transistors —as Fig. 4 shows—, keeping the same capacitance and avoiding incompatibilities with standard RAM-dedicated fabrications process.

One important characteristic of the proposed alternative is the fact that it does not include additional complex hardware, using only slightly-modified cells. Also, dummy cells can be placed in specific memory locations where critical information is stored, or randomly across the whole memory. And It is important to highlight, the memory structure is not altered, reason why it is difficult for a hacker to find unusual hardware that arouses suspicions.

978-1-5090-5544-9/17/$31.00 ©2017 IEEE

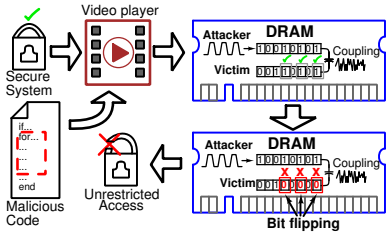

Fig. 1. Illustration of a DRAM Hammering attack

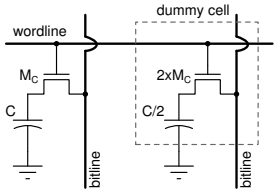

Fig. 2. Dummy cell with reduced capacitance and increased transistor size.

III. Results

A DRAM array was simulated in a 65nm CMOS standard technology. The purpose of this simulation is to prove the concept of accelerated discharge rate in a dummy cell. The simulated array consists of a 64×64 cells including a dummy cell per row similar to Fig. 3. Although a CMOS 65nm process was used, the results could be extended to a DRAM technology [5] considering that a 65nm CMOS performance reflects a state-of-art DRAM dedicated process [5]. Furthermore, the simulated array includes the RC coupling model, where each connection between cells uses a distributive model in each wordline.

The Fig. 5 presents a simulation of the discharge process of a victim row for a standard memory and a dummy cell under process and temperature variations. The aggressor row is being accessed with a frequency of 1GHz and one of the adjacent rows is being monitored. The threshold for memory controller alert is set to $V_{DD}/2$. The results show that always the dummy cell loses its charge with an increased rate, ensuring that capacitor voltage crosses the threshold before the standard cell one does. The crossing point for dummy cell is at least 1µs less than for the memory cell, and with a voltage difference about 300mV in the crossing point. This result is translated into a corrupted data in dummy cells with enough time in advance to a refresh cycle.

In order to validate the robustness of the proposed alternative, process variations were included in the simulation models for both coupling and interconnection resistance. The Fig. 6 shows the time difference between threshold crossing of dummy and standard cells. This difference varies from 0.5µs to 3µs, ensuring that the dummy cell crosses the threshold in less time than memory cell. Moreover, the voltage difference between capacitors of both types of cells is about 300mV in all cases at the time of dummy cell crossing point, ensuring that the dummy cell is corrupted faster than memory cell.

It is important to highlight that the proposed strategy does not affect the memory normal operation. Even though the leakage current of the dummy cells is higher, the conditions to discharge its storage capacitor faster than a standard cell are proper of a malicious attack. In normal operation the memory refresh rate is smaller than capacitor discharge.

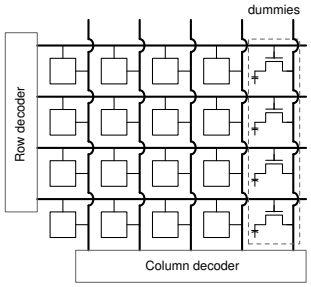

Fig. 3. Dummy cells within a DRAM array.

References

[1] Y. Kim *et al.*, in *IEEE ISCA*, June 2014, pp. 361–372.
[2] D. H. Kim *et al.*, *IEEE CAL*, vol. 14, no. 1, pp. 9–12, Jan 2015.
[3] D. Gruss *et al.*, in *arXiv*, 2016.
[4] D. Goodin, "Dram bitflipping exploits that hijack computers just got easier [online]."
[5] K. C. Huang *et al.*, in *IEEE IEDM*, Dec 2011, pp. 24.7.1–24.7.4.

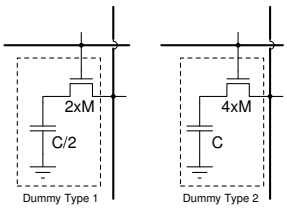

Fig. 4. Dummy cells within a DRAM array.

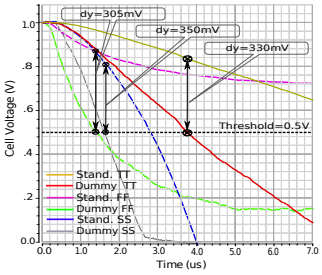

Fig. 5. Discharge process under the influence of coupling noised in a DRAM array.

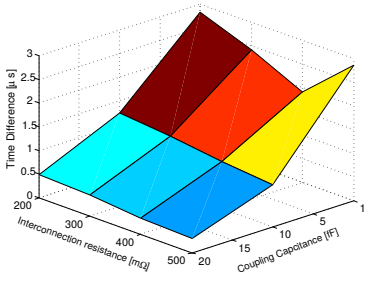

Fig. 6. Time difference between memory cell and dummy cell discharge.

978-1-5090-5544-9/17/$31.00 ©2017 IEEE