

Abstract

Computer Implemented Method for Preventing Rowhammer Attack in a Computing Device

5

A computer implemented method (200) for preventing rowhammer attack in a computing device is disclosed. The device has memory which includes a plurality of untrusted memory portions and a plurality of trusted memory portions, the plurality of untrusted memory portions and trusted memory portions being distributed within the memory. The method comprises: determining (202) respective trusted memory portions that are arranged physically contiguous to respective at least one untrusted memory portion to provide an identified set of trusted memory portions, the respective untrusted memory portions being accessible to perform the attack on the respective trusted memory portions; determining (204) trusted memory portions in the identified set of trusted memory portions that are movable to a different memory location in the memory; moving (206) the movable trusted memory portions to an available memory location in the memory to form a block of trusted memory portions; generating (208) at least one memory guard portion; and configuring (210) the memory guard portion to be arranged at an end of the block of trusted memory portions that is physically contiguous to an untrusted memory portion. The memory guard portion prevents electrical-interaction between the block of trusted memory portions and the untrusted memory portion to prevent the attack.

25 FIG. 2