Claims

1. A computer implemented method for preventing rowhammer attack in a computing device, the device having memory which includes untrusted memory portions, trusted memory portions and a first data portion, the untrusted memory portions and trusted memory portions being distributed within the memory, the first data portion accessible by a read-only function via the untrusted memory portion and accessible by a read-and-write function via the trusted memory portion, the method comprises:

(i) determining trusted memory portions that are arranged physically contiguous to at least one untrusted memory portion to provide an identified set of trusted memory portions, the untrusted memory portions being accessible to perform the attack on the physically contiguous trusted memory portions;

(ii) determining trusted memory portions in the identified set of trusted memory portions that are movable to a different memory location in the memory;

(iii) moving the movable trusted memory portions to an available memory location in the memory to form a block of trusted memory portions;

(iv) generating at least one memory guard portion;

(v) configuring 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, wherein the memory guard portion prevents electrical-interaction between the block of trusted memory portions and the untrusted memory portion to prevent the attack;

(vi) duplicating contents of the first data portion;

(vii) copying the duplicated contents to a second data portion in the memory, the second data portion configured to be isolated from the first data portion; and

(viii) configuring the first and second data portions to be accessible only by the trusted memory portion, and the untrusted memory portion respectively.

2. The method of claim 1, wherein the method is configured to be incorporated in a memory allocator and a bootloader of an operating system of the device.

3. The method of any preceding claims, wherein each trusted memory portion includes being secured against access by unauthorized software processes executed on the device.

4. The method of any preceding claims, wherein the memory includes dynamic random-access memory or NAND flash memory.

5. The method of any preceding claims, wherein the memory guard portion is configured to be devoid of data, or to include any data.

6. An apparatus configured to prevent rowhammer attack in a computing device, the device having memory which includes untrusted memory portions, trusted memory portions, and a first data portion, the untrusted memory portions and trusted memory portions being distributed within the memory, the first data portion accessible by a read-only function via the untrusted memory portion and accessible by a read-and-write function via the trusted memory portion, the apparatus comprising:

a first module arranged to determine trusted memory portions that are arranged physically contiguous to at least one untrusted memory portion to provide an identified set of trusted memory portions, the untrusted memory portions being accessible to perform the attack on the physically contiguous trusted memory portions;

a second module arranged to determine trusted memory portions in the identified set of trusted memory portions that are movable to a different memory location in the memory;

a third module arranged to move the movable trusted memory portions to an available memory location in the memory to form a block of trusted memory portions;

a fourth module arranged to generate at least one memory guard portion;

a fifth module arranged to configure 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, wherein the memory guard portion prevents electrical-interaction between the block of trusted memory portions and the untrusted memory portion to prevent the attack

a sixth module arranged to duplicate contents of the first data portion;

a seventh module arranged to copy the duplicated contents to a second data portion in the memory, the second data portion configured to be isolated from the first data portion; and

an eighth module arranged to configure the first and second data portions to be accessible only by the trusted memory portion, and the untrusted memory portion respectively.