| | | |
|---|---|---|
| | **Experiment title:**<br>Investigating smartcard security by time-resolved x-ray induced electronic perturbations | **Experiment number**:<br>ME-1411 |
| **Beamline**:<br>ID16B | **Date of experiment**:<br>from: 12 May 2016 to: 16 May 2016 | **Date of report**:<br>19/08/2016 |
| **Shifts:**<br>12 | **Local contact(s)**:<br>R. Tucoulou | *Received at ESRF:* |

**Names and affiliations of applicants** (* indicates experimentalists):

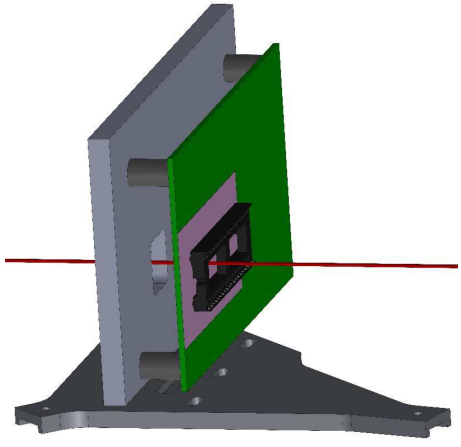
S. Anceau*, J. Clédière*, L. Maingault*, J-L. Rainard*, P. Bleuet* (CEA, LETI)

## Report:

This experiment aimed at performing non-invasive attacks on smartcard-like chips to perturb logic functions or internal memories behaviour. Usually, infrared laser-beams are used, but spot sizes and penetration depth can be a limitation to perform very local analyses of packaged components. The brilliant x-ray beams of the latest synchrotron nanobeamlines, just like ESRF-ID16B is, opened the way for the first time to new kind of x-ray induced attacks of microelectronics circuits.

To reach that goal, 12 shifts have been allocated on the ID16B beamline. From our experience using lab-systems (with spot size much bigger), it was decided to fix the energy to 17.5keV to make sure that a sufficient number of electron-hole pairs were created, while being sufficiently penetrating. The beam size at that energy was 63x57 nm (VxH) and turned out to be extremely stable during the 12 shifts. No beamtime loss due to beamline instrumentation of storage rings issues occurred.

The chips were mounted on large carriers which were vertically mounted thanks to a mechanical adaptor specifically designed for that (figure1, left). The sensitive surface of the chip could therefore be brought right in the x-ray focal plane. USB-communication between the chip, an in-house controlling computed and SPEC was efficient thanks to ESRF computing support.



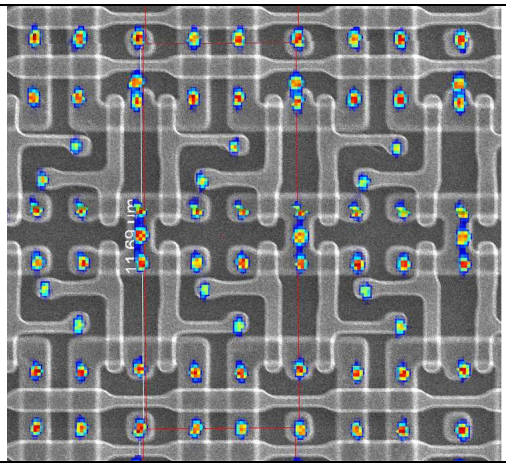


Figure 1 : Geometrical arrangement of the setup (left). Fluorescence map superimposed to ~~the visible light microscope available at the beamline (right) for localization~~ a MEB view of an etched device, showing vias and MOS transistors of RAM cells.

The first issue was to fix the dose, which was a critical unknown given the novelty of the experiment. It took us a bit of time to find the optimal configuration (basically good values for counting time and attenuator materials and thicknesses). In 16-bunch mode and with the proped attenuator configuration, few seconds were enough to create single, local faults.

Initially the chips were illuminated exclusively for x-rays attacks – no beam alignement was done before, to prevent from undesired memory switch. We then realized that is was possible to locate the transistors with chemical mappings, using the energy dispersive detectors available at the beamline. Therefore, raster scans of a region of interested were measured each time, paying attention to the dwell time to prevent from unexpected bit switch. Typically, 50ms dwell time was used. Then, on the fluorescence map, a specific transistor was selected and illuminated for a sufficient period of time to perturb the circuit (figure1, right).

~~A total of XXX samples were analysed, including (YYY) Flash, (ZZZ) RAM, etc. .~~ Several samples were analysed, including a microcontoller (for EEPROM and RAM experiments) and a NOR FLASH device. Important results include the fact that x-ray induced attacks on non-volatile EEPROM and NOR FLASH memories could be performed on a unique cell, at any previously chosen address, while this cannot be performed using IR-laser attacks. On RAM memories, the ID16B x-ray nanobeam ~~could switch bits from 0 to 1~~ can stuck a single cell at 0 or at 1, at any previously chosen address. ~~(and vice and versa),~~ Fault polarity (0 or 1) depends on which TMOS was irradiated in the cross-coupled inverters of the cell. ~~Compléter un peu…~~
The experiment was very successful and work is being done to promote results in a scientific paper. Also, it is planned to apply for a new period of beamtime in September 2016 to perform an in-situ study of the annealing effects to bring the bits back to their default values.