Scribe: Security and Privacy Threats to On-Chip Non-Volatile Memories and Countermeasures

Magnetic Tunnel Junction:

- How to change magnetization, that is, information?

Ans: Using spin current to accumulate magnetic field in the interface so as to change magnetization.

- How long does writing in magnetization takes?
- What the way the insulating layers/free layers tends to be tampered?

Ans: The strong external magnetic field applied to destroy or tamper the information stored in the magnetization as mentioned above. Specifically, STTRAM is susceptible to variations. The solution way is to increase its thermal stability, however, this method that will increase the latency of writing and read both. In addition, the longer latency gives attackers more opportunity to tamper or snoop information.

- If increasing flip time, the information or could be tampered easily.
- Temperature issues like if it is colder, tampering happens easily.
- Dynamic processing would increase temperature dramatically?

Ans: I think it probably happens. However, the writing must be controlled. The less writing , the less energy generated.

- ECL switching
- mixing STT and RRAM
- How to attack the magnetic torque systems like STT system?

Ans: attackers can distinguish writing states and reading states by the magnitude of current because writing needs more current than reading.

- Explain why retention makes reading and writing failure and how it happens?

High retention tends to fail writing process; Low retention have a large possibility of failure in reading.

- The difference of erasing and writing is not clearly known.
- Read modes is more susceptible than writing due to its vulnerability to the current (AC?DC?)
- Solutions: attack sensor is viable, which can detect the disturbance and then trigger protection acts. The sensors not only can be applied for magnetic field attacks but for temperature.
- Force STTRAM into retention mode when the intentionally attack is detected. But this way only slow down attacking but cannot entirely prevent from attacking.
- Semi-NVMs: take advantage of NVM's scalability, long retention, however, long retention let bits be vulnerable so the free layer in STTRAM can be reduced to decrease retention.
- How could you read that valid bits that are erased to prevent from being snooped?

The comment : attackers cannot take advantage of missing events to access data unauthorizedly due to the function of erasure.