Magnetic tunnel junctions can prevent tampering and piracy of intellectual property

April 3 2023

Credit: King Abdullah University of Science and Technology

Imagine a movie about a rogue employee who breaches security in a company that implants chips inside half of the world's computers. They embed a Trojan in systems around the globe and hold the world to ransom.

This is not unimaginable, says Rajat Kumar, a Ph.D. student in Yehia Massoud's lab at KAUST. "A single company currently supplies more than half of the world's chips, and nearly all of the most advanced chips," he confirms.

Massoud's group researches emerging technology that could make chips more secure. A recent project reports multifunctional logic gates that offer users a range of hardware security advantages. These include better control over their devices, tamper protection, watermarking and fingerprinting, and layout camouflage.

"Even if a semiconductor foundry is highly trustworthy, an untrusted entity in the supply chain could tamper with chips," Massoud says.

"If these were chips for a country's defense force, then a breach could affect that entire country's security."

Sourcing components from a long complex supply chain brings risks of classified chips being intercepted and reverse engineered, counterfeited or intellectual property being stolen.

As a secure alternative, Kumar and colleagues explored polymorphic gates made from nanoscale structures consisting of an oxide layer sandwiched between two ferromagnetic layers. These structures, known as a magnetic tunnel junctions (MTJ), are easily switchable by reversing the relative orientation of magnetic spins of the ferromagnetic layers. This spin-based control makes MTJs examples of spintronic devices.

Kumar and colleagues thought the switchable properties of MTJs meant that they could be used to create polymorphic gates, whose configuration users could check and reconfigure, overwriting any nefarious settings. They showed that MTJs function as polymorphic gates in a way that prevents tampering and intellectual property piracy due to their symmetry at both circuit and layout level symmetry, obscuring their layout and making them hard to reverse engineer.

MTJs are used in hard drives, opening the possibility for combining memory and processing functionality, which could drastically reduce the

power consumption and delay of interconnects. MTJs cannot yet match the functionality of conventional chips, because their output driving capability is not as high.

Others are exploring different emerging technologies for hardware security potential, but Massoud believes spintronic devices will play a significant role. "They are energy efficient and nonvolatile and are easily integrated with conventional silicon substrates," he says.

More information: Rajat Kumar et al, Polymorphic Hybrid CMOS-MTJ Logic Gates for Hardware Security Applications, *Electronics* (2023). DOI: 10.3390/electronics12040902

Provided by King Abdullah University of Science and Technology