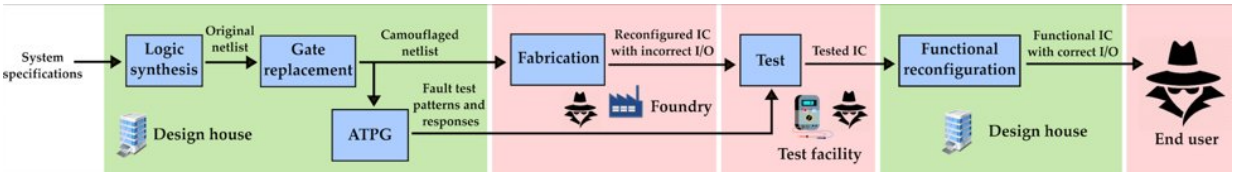
A dynamic camouflaging approach to prevent intellectual property theft

November 27 2018, by Ingrid Fadelli



The globalization of the IC supply chain has induced vulnerabilities at various stages of IC production. Here, the red zones stages are untrusted and can be exploited by an attacker. Credit: Rangarajan et al.

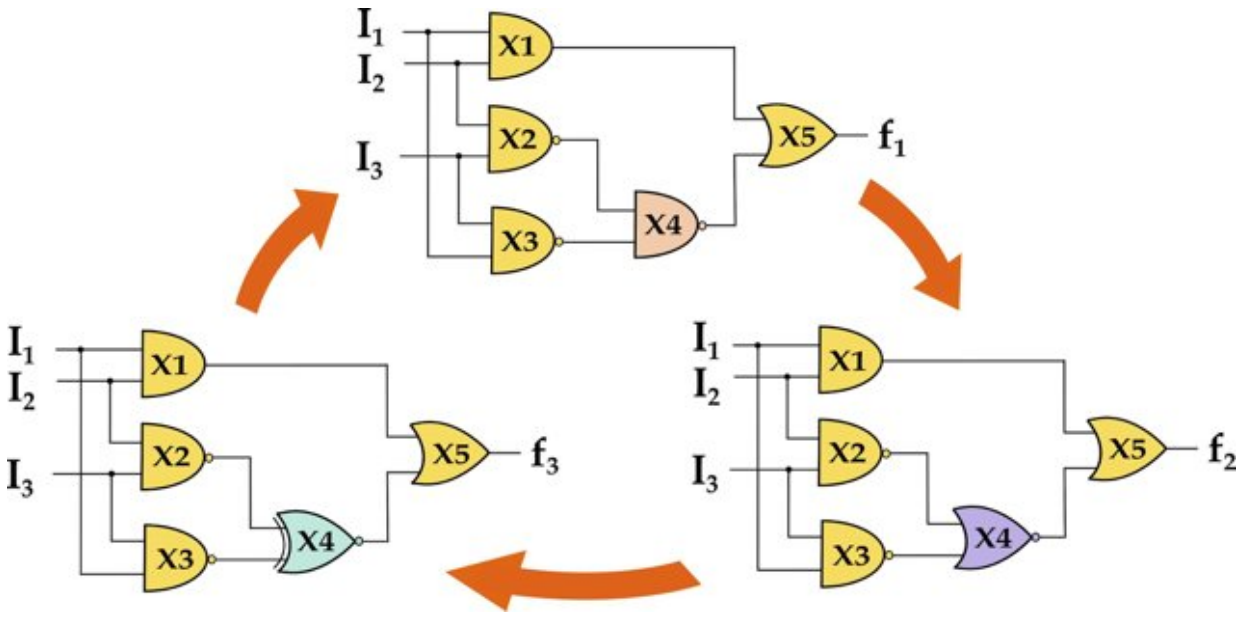
In recent years, hardware-centric security threats have emerged at different stages of the integrated circuit (IC) supply chain. This has enabled the proliferation of various malicious attacks, such as intellectual property (IP) piracy, illegal overproduction of ICs, and insertion of hardware Trojans.

Out of all existing defenses against IP piracy, only logic locking has so far been found to offer effective end-to-end protection. To address these challenges, a research team at the New York University Center for Cybersecurity and Quantum Nanoelectronics Lab has developed a dynamic camouflaging approach to thwart IP reverse engineering at all stages of the supply chain.

"The globalization of the integrated circuit supply chain has resulted in

the outsourcing of various steps of the microelectronic chip production," Nikhil Rangarajan, one of the researchers who carried out the study, told *TechXplore*. "Chips are typically designed and/or procured from one country, fabricated in another, and finally tested and packaged elsewhere. This worldwide chain opens up lot of opportunities for attackers to steal the underlying IP, indulge in overproduction, or even insert malicious modifications known as hardware Trojans."

According to estimates, the semiconductor industry loses billions of dollars every year due to IP theft. To mitigate this damage, the research carried out by Rangarajan and his colleagues specifically focuses on preventing IP theft.



Dynamic switching of polymorphic circuits on-the-fly. Credit: Rangarajan et al.

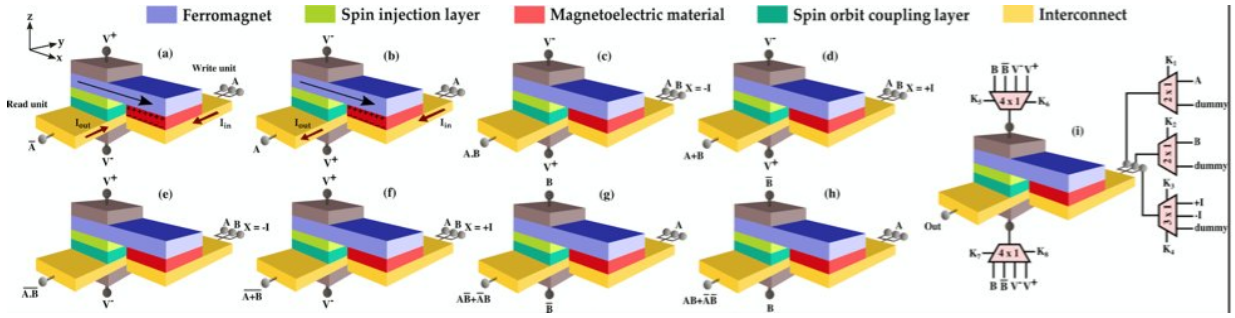
"The inspiration for our idea came from nature, where some animals like

octopus are able to change their physical appearance to adapt to their environment to avoid detection by prey or predators," Rangarajan explained. "We thought: Why can't the electronic circuits we seek to protect also change dynamically to avoid detection by an attacker?"

Existing defense mechanisms for the prevention of IP theft, such as static camouflaging, require the designer to trust the foundry commissioned for the chip's fabrication. On the contrary, the threat model devised by Rangarajan and his colleagues assumes that an attacker might also reside within the foundry or in the test facility, or could potentially be an end user.

"By using innate properties like polymorphism, multi-functionality, and post-fabrication reconfigurability offered by emerging spintronic devices, such as the magnetoelectric spin orbit (MESO) device, we were able to achieve dynamic camouflaging," Satwik Patnaik, another researcher involved in the study, told TechXplore. "Polymorphism is intended in the particular means through which the device can readily implement different Boolean functions at runtime, where the functionality is determined by an internal or external control mechanism."

In the scheme devised by the researchers, a potentially malicious foundry fabricates the logic gates as "black boxes," which can only be configured by the designer once the fabrication process is complete. This prevents an attacker within the foundry from deciphering the intended functionality of the chip that is under fabrication, as it is yet to be configured.



Dynamic camouflaging is possible with the help of novel spintronic gates like MESO gates. These gates can implement several Boolean functionalities in one device and can also switch between them during runtime. Credit: Rangarajan et al.

"This 'post-fabrication re-configurability' property also enables protection from untrusted test facilities, as the chip can be configured for any dummy functionality unknown to an attacker and restored to the true functionality once the testing has been carried out," Patnaik explained. "In short, while prior works in IC camouflaging are static and have to trust the foundry, our scheme doesn't require the designer to trust the foundry or the test facility."

The researchers evaluated the effectiveness of their approach in counteracting state-of-the-art test-data mining attacks, such as HackTest, and side-channel analysis, where adversaries aim to decipher the IP's functionality. They also explored its performance with powerful Boolean satisfiability attacks, including SAT and approximate SAT (AppSAT), which are typically preferred by end-users.

Their dynamic camouflaging approach yielded promising results in all these tests. In the future, the researchers believe that it could help to thwart attackers within untrusted foundries or test facilities.

"Our scheme leverages the unique properties of spin-based devices," Rangarajan explained. "These properties, especially polymorphism, cannot be afforded by current-day CMOS technologies, due to the fundamental limitations of CMOS devices. We also want to emphasize that the general notion of dynamic camouflaging could be implemented with other emerging devices, as long as they have similar properties."

Input $I_1I_2I_3$	Oracle output $f_1f_2f_3$	Current oracle	Output for different key combinations								Inference
			k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	
000	001		0	1	1	1	0	0	0	1	
001	001		0	1	1	1	0	0	0	1	
010	001		0	1	1	1	0	0	0	1	
011	100	f_2	1	0	0	1	1	0	1	0	iter 2: k_0, k_3, k_4, k_6 pruned
100	001		0	1	1	1	0	0	0	1	
101	100	f_1	0	1	0	1	1	0	1	0	iter 1: k_0, k_2, k_5, k_7 pruned
110	111		1	1	1	1	1	1	1	1	
111	111		1	1	1	1	1	1	1	1	

A Boolean satisfiability attack mounted on a dynamically camouflaged circuit can easily yield an incorrect key and mislead the attacker. Credit: Rangarajan et al.

To promote the implementation of their defense technique, the researchers also envision a hybrid CMOS-spin based integration. This integration could facilitate the adoption and acceptance of their scheme, as well as of devices that support it. According to the researchers, several academic studies are currently heading in similar directions.

Rangarajan and his colleagues are now planning to investigate the

implications of using run-time polymorphism to protect approximate logic circuits, which have been gaining a lot of traction over the past few years. These types of circuits trade off output accuracy for a steep reduction in power dissipation.

"Especially with the advent of the Internet-of-Things (IoT), we believe that the protection of approximate computing chips is also essential, given the fact that they are widely favored to be used in systems that require low power operation," Rangarajan said. "We also plan to evaluate the resilience of our scheme under other attack scenarios, to gain further confidence in our approach."

More information: Opening the doors to dynamic camouflaging: harnessing the power of polymorphic devices. arXiv:1811.06012 [cs.CR]. arxiv.org/abs/1811.06012