# Microchip fingerprints used to lock out chip pirates

March 11 2008

Pirated microchips -- chips stolen from legitimate factories or made from stolen blueprints -- account for billions of dollars in annual losses to chipmakers.

But a series of novel techniques developed at Rice University over the past year could stop pirates by allowing chip designers to lock and remotely activate chips with a unique ID tag. When a chip is locked with the new technology, only the patent-holder can decipher the key and activate the chip -- meaning knockoffs and stolen chips are worthless.

"Ours is the first remote-activation scheme that protects integrated circuits against piracy by exploiting their inherent, unclonable variability," said the technology's original inventor, Farinaz Koushanfar, assistant professor in electrical and computer engineering at Rice. "We use slight variations that arise in modern manufacturing to create a unique, digital identification that acts like a fingerprint for each chip, and we integrate that into the chip's functionality."

The original work was presented last August at the USENIX Security Symposium in Boston. Since the invention of the method, Koushanfar has collaborated with a number of researchers to build upon her original scheme. Last October, at the International Conference in Computer Aided Designs, Koushanfar and Rice graduate student Yousra Alkabani, in collaboration with Miodrag Potkonjak from UCLA, showed the first method that could continuously check, control, enable and disable a chip's operation online by integrating the chip's fingerprints into its

functionality and actively checking them during operation.

This month, Koushanfar and colleagues at the University of Michigan, Igor Markov and Jarrod Roy, unveiled a new form of the technology called “EPIC: Ending Piracy of Integrated Circuits" at the IEEE Design Automation and Test Conference in Europe. The latest method is based on public key cryptography and works for chips that already have a built-in cryptography module. In all tests and research published during the past year, the new technology has proven to be stable, unclonable and attack-resilient.

"The public tends to overlook hardware piracy and focus instead on the well-known and oft-publicized problem of software piracy," Koushanfar said. "But some intellectual-property experts who have studied both estimate that the economic losses from hardware piracy is more severe compared to software piracy."

Hardware piracy has become increasingly problematic as the skyrocketing costs of microchip production have led chip-design companies to get out of the manufacturing business. When design and manufacturing are done by different companies, the design company's sole asset is the intellectual property (IP) associated with the integrated circuit's (IP) blueprints.

Hardware makers have tried a number of approaches to safeguard designers' IP, including stamping chips with watermarks, registering legitimate chips in databases and requiring the one-time use of an ID to unlock a chip's functionality. But safeguarding individual ICs – and not IPs – is the unique aspect and contribution of Koushanfar’s work.

Koushanfar said her original technology and her subsequent collaborative work stand apart from previously tried schemes because the ID generated in her scheme is derived directly from the chip itself,

and without the ID, the chip will not function.

"The chip itself provides the key," she said. "There is no way to steal it because it doesn't exist until the chip is actually made, and once made, only the designer knows how to decipher the key."

For her original invention, Koushanfar has received the Defense Advanced Research Projects Agency (DARPA) Young Faculty Award last year. Both the National Science Foundation and DARPA presently fund Koushanfar's research. Koushanfar is also the director of the Texas Instruments DSP Leadership University program at Rice and has close industrial-level collaborations on her hardware security projects.

Source: Rice University