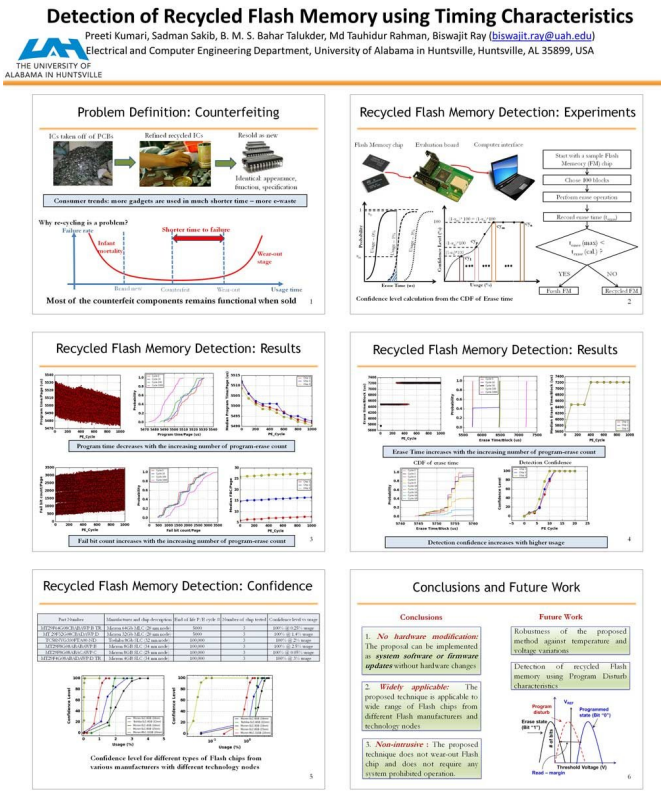
Researchers develop novel technique to identify counterfeit flash memory

30 May 2018, by Diana Lachance



The team presented their research at the 2018 IEEE International Symposium on Hardware Oriented Security and Trust, which was held from April 30 to May 4 in Washington, D.C. Credit: University of Alabama in Huntsville

Counterfeiting electronic components may sound like a plot point lifted from a technothriller by Daniel Suarez or Michael Crichton, but it's a very real – and growing – threat to the safety and reliability of our critical infrastructure.

"Nowadays we use consumer electronics for a year or so, but the components in them remain 'alive' for up to 10 years," says Dr. Biswajit Ray, an assistant professor in the Department of Electrical and Computer Engineering at The University of Alabama in Huntsville (UAH). "As a result, there's an incentive to bring them back to market by harvesting them from scrapped printed circuit boards and re-using them in spite of the adverse effects that these counterfeit components can have because of their limited endurance."

The problem has been further exacerbated in recent years as the semiconductor supply chain has shifted from a vertical to a horizontal model. "Because of manufacturers' enhanced reliance on independent suppliers," says Dr. Ray, "these electronic systems are at a lot more risk of counterfeiting and piracy than ever." And as counterfeiters get more and more savvy, it can be harder and harder to tell whether the components in any given electronic system are fresh or recycled – that is, he says, "until they stop working and the consumer blames the manufacturer for making a faulty product!"

At particularly high risk of counterfeiting is flash memory, a nonvolatile digital storage medium that stores data on a chip. "Flash is a major target because of its presence in the most electronic systems – it's used for everything from space applications to consumer electronics," says Dr. Ray. "But detection of recycled flash with high confidence is challenging due to the variability among different flash chips." Few feasible solutions have been proposed, however, and those that have rely on the maintenance of an extensive database or on manufacturers' willingness to adopt sensor-based approaches.

Until now, that is. Together with his colleague Dr. M. Tauhidur Rahman and graduate students Preeti Kumari, M.S. Bahar Talukder, and Sadman Sakib, Dr. Ray has developed a novel method of detecting counterfeit flash memory based on a combination of the statistical distribution of various timing characteristics of memory and the number of faulty bits.

"Most researchers focus on fail bit count or how fast the chip can read and write – they never worry about program-erase time," explains Talukder of the team's approach. "But while fail bit count and read and write time do show changes, program-erase time is the best metric because it shows the most amount of variation." It's also more consistent across manufacturers and tends to increase noticeably even after just a few program-erase cycles. "We found that we were getting a 100 percent confidence level – a decision metric that measures whether we can detect a recycled memory accurately – for a flash with just 3 percent usage," says Sakib. Just as important for any future consumers, the technique is "inexpensive, non-destructive, and requires no additional hardware," says Kumari, who is now looking into testing it against temperature and voltage variations.

The team has already filed several patent applications to protect their detection method, which they hope to one day turn into both a smartphone application and a browser extension. But far from hoping to profit personally from the endeavor, they're more interested in helping safeguard the electronic systems used by our nation's most vital infrastructure sectors. "Failure of flash memory in critical applications can have catastrophic effects, from simply corrupting the system to enabling a hardware Trojan attack," says Dr. Rahman. "So there is a big demand for this ability to detect counterfeit flash with high confidence."

Provided by University of Alabama in Huntsville