Shorted circuits: Foiling microelectronic counterfeiters with evidentiary DNA

James A. Hayward, Ben Liang, Janice Meraglia, and Alex Tran
Applied DNA Sciences, Inc., USA

The global tsunami of counterfeits in recent years has turned to semiconductors (SC), brewing a "perfect storm" of risk to high-reliability users in medical devices, communications, defense and other industries. Counterfeit electronic components pose a special threat to industry and government. In recent years, the global supply chain has diversified and outsourcing of sub-systems, assemblies, sub-assemblies, and components is now the norm.

The US disposes its electronic rubbish in Asia, where it is often disassembled and electronic parts are recovered, recast and relabeled as original new parts (usually bearing no relationship to the original, functional part). Today, a counterfeit chip can too easily pass visual and other inspections even if functionally the chip has no relationship to its labeled identity. The relabeled parts (now "counterfeit") flood the US market, stealing up to one third of legitimate sales. These counterfeit parts put every electronic assembly at risk of failure. In some cases (weapons, fighter aircraft, communications equipment), failure can come with catastrophic consequences. Worse, counterfeit microchips sometimes are accompanied by preloaded malware, posing the threat of cyber attack.

DNA evidence is accepted as the gold standard of evidence in courts globally, and it has survived thousands of challenges since first being introduced as evidence in 1980.

We have developed a system of engineered forensic marks, derived from rearranged botanical genomes and combined with sensitive chemical reporters. These DNA taggants may be applied to a wide variety of media, including currency. Unlike other anti-counterfeiting marks, these DNA tags cannot be copied by counterfeiters, as proven by federal agencies. The UK Metropolitan Police Service and the Stockholm police have utilized DNA tags as key evidence in the convictions of more than 30 criminals, resulting in over 150 years of jail time.

The Defense Logistics Agency, the procurement arm of the Department of Defense, has been investigating the feasibility of marking electronic components with a secure DNA marker as part of the manufacturing process. The initial viability study was so successful that the agency embarked on a broader, more robust program. This current effort spans the entire microcircuit supply chain and engages leading industry participants. The DNA tags are small enough to be placed in various covert locations on a chip, all the way down to the silicon wafer.

If the authenticity of a single component or batch is suspect, rapid screening tests may be complemented by full forensic analysis to prove point of origin.

Counterfeiting technologies and their economic impact will be reviewed. The results of recent, large-scale trials to prevent counterfeits in supply chains will be presented. Chemical and physical methods for marking microelectronics will be discussed.