What's in a chip?
The answer may dent the profits of a company – or compromise a nation's military might.

Top-Secret Circuitry

Computing and communications have long depended on the technological infrastructure of semiconductors; increasingly, the nation's economy and security rely on silicon chips as well. It follows that the security of these chips (integrated circuits, or ICs) has become a vital concern.

Many chips contain highly specialized technology or perform proprietary functions. Mapping out the circuitry on these chips could reveal industrial secrets to a rival manufacturer or undermine the effectiveness of a critical military device. Even worse, an adversary with full understanding of a chip's circuitry might implant "rogue" elements to cause malfunctions or create vulnerability. This paper discusses the use of 3D-IC technology to enhance the security of sensitive electronics.

Reverse Engineering

Reverse engineering is the examination of an existing device, object, or system to discover its contents, structure, and function. This is a useful process in commercial electronics. If one component of a product becomes obsolete, or if the component's vendor goes out of business, the entire product faces a costly redesign. To avoid this, the obsolete component can (with appropriate tools and skills) be reverse engineered in order to replicate its functionality. A single part is replaced, and the rest of the product remains unchanged.

To reverse engineer an IC, the silicon-based chip is typically taken out of its housing and etched to remove the top layers of metal, making the circuitry visible. An experienced engineer can then visually identify much of the circuit and deduce its functions. Additional layers of the circuit may be etched away to reveal lower layers, but because the de-layering process removes different materials at different rates, the result becomes increasingly imprecise with each layer. Reverse engineering a highly complex IC might require a team of skilled engineers performing tests on a large number of chips.

A more sophisticated (and expensive) way to decipher an IC is by reading its voltage during operation. Specialized equipment can image and record the changing voltage in a live circuit to create a "movie" of its behavior. The images can be analyzed to disclose the chip's circuitry and even reveal the contents of on-chip RAM.

Reverse engineering can be a benign activity, but it can also serve as a malicious espionage tool to decrypt sensitive electronics in either industrial or military situations. A quick search of the US Patent database reveals hundreds of patents designed to prevent the reverse engineering of integrated circuits.

Security in Manufacturing

Reverse engineering is not the only threat to a chip's security. The design itself may be vulnerable to theft and/or sabotage during creation, storage, transfer, or manufacturing. Data security is an ever-growing concern. Commercial entities and government agencies alike take great care to secure their computers, their facilities, and their communications. When a chip is ready for manufacture, handing the design over to a fab (semiconductor wafer foundry) requires a high level of confidence in that fab's security as well.

The U.S. government has a DoD-NSA program in place with stringent criteria by which a fab can be rated as a "Trusted Foundry." A fab rated as "Trusted" is very much in demand for sensitive products,

commercial as well as military. Not surprisingly, the coveted “Trusted” rating is difficult to obtain, especially for foreign foundries. Some of the biggest and best fabs are therefore not eligible to perform sensitive manufacturing, and customers may find themselves sacrificing economy and/or timeliness in the interests of security.

3D-ICs

An exciting new development in IC manufacturing is the Three-Dimensional Integrated Circuit (3D-IC), a single circuit built by stacking and integrating separately-built layers. Although the technology is chiefly noted for its increased density, speed, and power conservation, it also offers unique security advantages.

With rare exceptions, the layers of a 3D-IC are manufactured on separate substrates and then stacked. Each substrate is aggressively thinned. The entire circuit is integrated by through-silicon vias (TSVs) that run vertically through the substrates from one circuit layer to another.

Defeating Reverse Engineering

The first security advantage of a 3D-IC is that the stacking process conceals much, if not all, of the circuitry. Assuming that the bottom layer of the stack is face-up and the top layer is face-down, the outside surface of the finished chip is completely blank except for I/O pads. (See photos at http://www.tezzaron.com/about/PhotoAlbum/Products/3D_Sensor.html)

The stacked structure effectively thwarts most attempts at reverse engineering. Prying the layers apart would destroy the circuitry. De-layering is theoretically possible, but etching evenly through the substrates would be extremely difficult. Voltage imaging would still be of use, but the many layers of wiring would produce a confusion of overlapped images, and the bond material and substrates would be likely to blur and attenuate the signal significantly.

Security in Manufacturing

The second security advantage provided by 3D-ICs is more subtle. A multi-layer circuit may be divided among the layers in such a way that the function of each layer becomes obscure. Assuming that the TSV connections are extremely fine and abundant, elements can be scattered among the layers in apparently random fashion. The missing pieces of the puzzle are layers of wiring, laid down just before bonding, that interconnect the jumbled elements into a functional device.

The beauty of this scheme is that manufacturing can be done at any fab, trusted or not, because the circuit layers are incomprehensible. For even more security, each layer could be built at a different fab. A “Trusted Foundry” would be needed only for the alignment and bonding steps, with their secret layers of wiring. To add an extra layer of concealment, the layers could be designed for offset alignment. This would connect the elements in non-obvious ways from one layer to the next. By taking advantage of these capabilities, chip designers can frustrate any attempt to decipher or sabotage the circuitry during manufacture.

Conclusion

Maintaining the security of sensitive circuitry is a high-priority matter. Attacks by hostile parties can be expected to increase in sophistication. As new methods are developed for detecting and neutralizing threats, 3D-IC technology represents an innovative and powerful tool in the defensive arsenal.