SEMICONDUCTOR ENGINEERING

Securing Chips During Manufacturing

Can directed electron writing change the security equation?

JULY 7TH, 2016 - BY: **ED SPERLING**

David Lam, chairman of Multibeam, sat down with Semiconductor Engineering to talk about how next-gen lithography tools can be used to prevent cyber attacks and counterfeiting of hardware.

SE: How did you get into the anti-counterfeiting business?

Lam: About three years ago we were working with some customers that were troubled by the counterfeiting problem. We became aware of that sense of urgency throughout business and government. We were doing CEBL (complementary e-beam lithography) at the time, and we still do that. And in the process we figured out a way to insert chip ID during production, with very little effort or additional time or cost. So that became part of the capability of our offering.

SE: And where does that fit into everything?

Lam: The IoT became very visible in the past 18 months. If you think about it, the attack surface is huge. Every Internet connecting point to the IoT could be a potential open door for cyber attacks. So we continued to work on it beyond chip ID.

SE: Where does this get inserted into the flow?

Lam: Customers seem to prefer it at Via 2 or Via 1. These via holes are really to create the security information deep inside a device.

SE: How do you work this in?

Lam: First, it doesn't matter if it's a mature node or advanced technology, or a 2D conventional layout or a 1D lines and cuts layout. It also doesn't matter if its 200mm or 300mm wafers. Most IoT devices rolling out are not using advanced nodes, but at about 50 nanometers. The key distinction here is that the directed electron writing (DEW) technology is not lithography. It's security. The foundry, working with its customers, decides at which layer it wants to insert that information and what you want to insert. Then the DEW writer will follow the security database to determine what information to

embed. A wafer will then go through one round of etching, and then back to the production line and finish.

SE: Let's talk about the sequence of steps. How does this work?

Lam: The foundry's customer would first decide what to embed and where. So when they design the chip, they would allocate space for this embedding of unique information in each chip.

SE: How much space are we talking about?

Lam: Very little. You're talking about the chip ID, which is a number, a MAC or IP address, and privacy key encryption. The encryption key is the most important thing for secure authentication. When the DEW writer is on the market, people will come up with different ways to use it because there are a lot of encryption experts out there. Now, in DEW writing, the wafer gets moved from the production line to the DEW writer, which patterns via holes to create the information at the location allocated for it by the designer. DEW employs lithographic techniques to accomplish the writing. That means you would spin-coat the wafer with electron resists and then do directed electron writing. After that, the wafer would go through typical steps like develop, etch, clean, and then go back to the production line.

SE: This cannot be done later?

Lam: Today, it is done after the device is finished, using lasers or electrical methods to burn fuses to write security information on a chip. But there are flaws in this approach. Most of these fusing operations are outsourced. The secret information you create is exposed, and the security is compromised. Second, it can be changed by someone who is determined to change it. Because of that it doesn't provide the security level required. If you embed the secret code in one of the layers deep inside the IC, then it's not visible or accessible from outside. You do want the ID to be readable from outside, so you allow access from the memory bus. But you cannot alter it. That's the important thing. And the encryption key is "private". If someone wants to slice open the IC to see what's there, they probably could. But the chip is guaranteed to be destroyed and each device has a different number. It's chip-specific and embedded.

SE: Are these random numbers?

Lam: Yes. Using the DEW technology, you can even put a random number generator inside the encryption engine of an SoC. There are different ways to generate encryption keys, such as prime numbers, elliptic curve cryptography. DEW is Switzerland. It's an enabling technology for implementation regardless of the encryption technology employed to generate the key. Once generated, you can allow access from other parts of the chip or it can be isolated.

SE: If someone gets a batch of chips, how do they know it's not counterfeit if you can't see the number?

Lam: At the test phase you can confirm it all. The chip ID can be read and you can interact with the MAC address. But you can't change these IDs. You can also send encrypted information into the device and let it decrypt that information. And all of this can be done very fast.

SE: So where do you go next?

Lam: After we finished the chip ID task, we began thinking about other things we could write to contribute to better security. We were talking with security experts and they said security has been around for a long time, but it's still not good enough to stop cyber attacks. They said we make chips, but we don't have anything to defend it. If you look at an IoT device, it has a microcontroller with very little memory and very few system resources. There is no security software to fend off a cyber intrusion. But we can insert something to make it safer. The ID that enables anti-tampering and supply chain anti-counterfeiting is very valuable, but the encryption adds another level of security. All the critical infrastructure have embedded within them programmable logic controllers (PLC). Like an IoT device today, the PLC is a simple microcontroller with minimal processing and memory and communication with SCADA (supervisory control and data acquisition) system. The SCADA system is located in the control center and remotely monitors the infrastructure, collects real-time data and adjusts PLC settings. If the IC in the PLC is embedded with security, changing the value of the PLC will require authentication and authorization, thus enhancing its defense against malicious intrusion.

SE: How does this compare with software security?

Lam: It complements software security and enhances cyber defense. In a car there may be as much as 100 million lines of code. Even though they separate the DVD player from the rest of the car, a hacker can still come in through other parts of the system. It's very vulnerable. So IoT may be the first application to launch IC-embedded security, but it's not the last. Automobiles will be next. Programmable logic controllers embedded in all of these infrastructures need better security, too.

SE: This changes the dynamics of the supply chain, as well, because it happens at manufacturing. So what's required to make this happen? An e-beam writer?

Lam: People have long dismissed electron-beam writing as a useful production tool. This is because they have targeted the wrong application. The first misguided application was to replace optical lithography with a totally maskless approach. That's why we focused on CEBL, which only patterns line-cuts and holes to complement optical lithography. The DEW application for security embedding is not next-generation lithography. It's writing via holes in each chip, independent of production. Maybe finally we are using electrons for the right thing – doing crucial tasks no other technology can, lithography or not.

SE: Can this be driven down to the IP block level, as well, for 2.5D or fan-out packaging?

Lam: Yes. We're working with leading EDA design IP suppliers to make it easy for the designers to implement. We are talking to established equipment companies, too.

SE: Why can't other lithography be used for the same kind of approach?

Lam: Optical lithography is the industry's workhorse, but each circuit layer must be printed through a mask in a cookie-cutter fashion. So every chip would have to be identical because it is done through the same mask. That's great for volume production, but it's not great for embedding chip-specific information. You have to be able to direct the electrons to where there is a specific hole to write in each chip. In other words, no mask-based technology can do this.

SE: How many writers do they need at a giant foundry doing billions of chips a year?

Lam: The goal is to match the production need. A multiple-column array spans the entire wafer, whether it's 200mm or 300mm. And the wafer is moved by a high-precision stage. We call it the electron writing module. Thanks to our invention of miniature multi-column array, the writing module is about the size of an etcher, so it can be readily integrated in a small cluster tool. A few DEW cluster tools would meet the requirement of a production line.

TAGS: 2.5D COUNTERFEITING E-BEAM E-BEAM INITIATIVE E-BEAM LITHOGRAPHY ETCH FAN-OUT IP MULTIBEAM SECURITY

Ed Sperling

Ed Sperling is the editor in chief of Semiconductor Engineering.