Add Security And Supply Chain Trust To Your ASIC Or SoC With eFPGAs

Using design obfuscation to keep confidential designs confidential.

BY: **RALPH GRUNDLER**

Before Covid-induced supply chain issues affected semiconductor availability and lead times, concerns about counterfeit parts and trusted supply chains were becoming the subject of many articles and discussions affecting critical data centers, communications, public infrastructure, and facilities such as regional power plants and the grid. Today's semiconductor design and manufacturing is complex, requiring touchpoints in many stages of development and gone are the days where the entire design stays in-house from design conception to manufacturing, packaging, test, and distribution. Even though there are many security and encryption techniques designers can use to make a chip secure, what else can be done to increase the confidence that the chip is trustworthy? eFPGA opens a new range of capabilities.

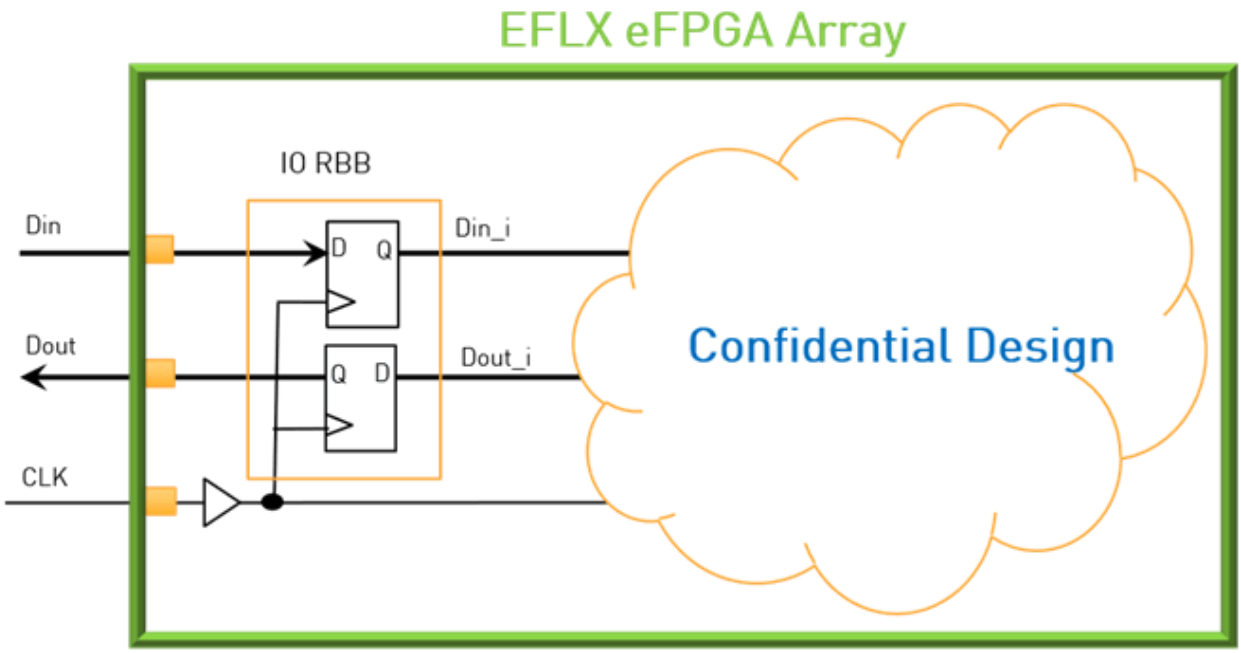
One issue with today's modern design flow is the access to "Trusted Fabs" for confidential designs. Just too many eyes in the process flow to assure that a confidential design can be kept confidential. Some would say this is a crisis for accessing fabs below 14nm.

In an effort to establish an entire supply chain that can be trusted, the United States Department of Defense (DoD) set up the Trusted Foundry Program as noted in this article: "People in the aerospace and the government communities want to get embedded FPGAs," said Geoff Tate, chief executive of Flex Logix. "But they want

them built in the U.S. They want finFET-class performance, so that leads you to GlobalFoundries. Being in the U.S. seems to make them feel comfortable. One issue, of course, is assurance of supply."

Unfortunately, this limits the processes available to the DoD and companies who need semiconductors from a trusted supply chain. Design obfuscation using eFPGA and other tools are providing solutions for customers seeking foundry independence, regardless of fab location.

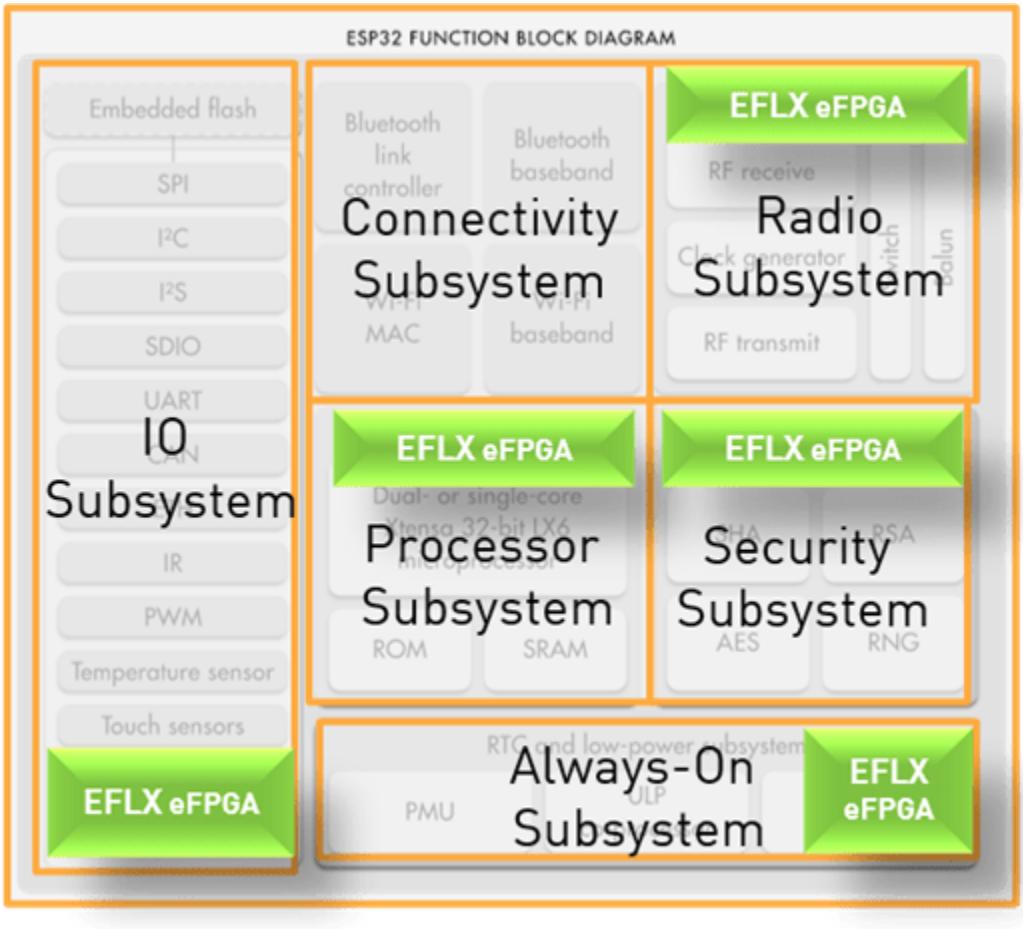
There are many articles written on FPGA and security, including "Are FPGAs More Secure Than Processors?" as a detailed description of the different security solutions that FPGAs (and eFPGAs) can provide. One solution that is quite simple and is generally described as obfuscation: add eFPGA to the SoC and program the confidential parts of your design after manufacturing in a trusted environment as shown in the diagram.



To safeguard against counterfeit parts, which typically consists of recycled, cloned or overproduced/failed parts, obfuscating a portion of the ASIC's circuitry in eFPGA can act like a car key that starts a car. Simply program the eFPGA as part of the ASIC's pre-boot sequence. If the eFPGA design "fits", then the circuits are completed and the ASIC continues to boot as normal. If not, then the ASIC is a brick. In this case, obfuscation is used as an electrical watermark.

Although the picture previously gives a good idea of what can be done with an eFPGA inside a SOC, what if you have more than one location that needs security?

eFPGA can be used within an IP block itself for specific security requirements. For example, a set-top-box ASIC could use eFPGA to manage content enablement in the transport block with proprietary code unique for each cable operator. The semiconductor manufacturer only has to produce a single ASIC that can be customizable in hardware post manufacturing by programming the eFPGA specific for each cable operator's requirements.



The same concept could be applied to streaming services and TVs to add an additional hardware encryption key check above what is currently being done in software alone. Another example are SSD controllers. Efficient LDPC encoding/decoding typically requires specific information about the NAND memory in the SSD drive which flash manufacturers are reluctant to provide because it

contains proprietary information. An SSD controller that can be programmed with an optimized LDPC algorithm for any NAND memory would provide the best performance while protecting sensitive information from the memory manufacturer.

With the reconfigurable nature of eFPGA, encryption keys that have been hardcoded in ASIC gates can now be changed post-manufacturing. Being able to dynamically change hardware license keys, like the way RSA tokens provide rotating codes, provides a temporal security measure at the hardware level. Combining this capability with PUF generated key as a handshake would make it virtually impossible for anyone to clone an ASIC.

While integrating FPGA on-chip has significant cost and power benefits, using smaller eFPGAs throughout an SoC can safeguard proprietary information and build supply chain trust through obfuscation and reconfigurability keeping hackers at bay. Next time you need secrecy think eFPGA.

eFPGAs have many additional benefits you can read about here, or you can just read what customers say here.

Ralph Grundler

Ralph Grundler is the senior director of marketing and architecture solutions at Flex Logix.