Use Triple DES for Ultimate Virtex-II Design Protection

Learn how to protect your intellectual property from piracy with encrypted bitstreams using on-chip decryptors.

by Michael Peattie
Product Applications Engineer, Xilinx Inc.
mike.peattie@xilinx.com

The Virtex®-II architecture provides hardware designers unprecedented design capabilities, but until now, designers had no way to protect their IP (Intellectual Property) from being cloned. Current FPGA technology requires the device to receive its configuration data from an external source. This makes it easy for a pirate to analyze or clone a design by tapping the configuration pins and storing the design configuration for use elsewhere.

Now, however, new Virtex-II devices have on-chip decryptors that have their keys loaded during board manufacture in a secure environment. Once the devices have been programmed with the correct keys, the devices can be configured with encrypted bitstreams. You can use random keys or choose your own.

Xilinx software encrypts bitstreams using the powerful Triple Data Encryption Algorithm. Triple DES is the standard employed by the United States government for secure communication and by banks around the world for money transfers. Both DES and Triple DES are now available in Virtex-II devices. Using three 56-bit keys makes a design virtually impenetrable.

How to Encrypt Bitstreams

Encryption is elegantly simple. First, you enter and simulate your design as you normally would. In the last step of implementation (BitGen), you set options that tell the software to encrypt the bitstream and what keys to use. This creates a special key file. The Xilinx JTAG Programmer uses the key file to program the keys in the Virtex-II device. Once the keys are in place, you can load bitstreams encrypted with your keys.

On the other hand, you don't need security, you can configure the device with non-encrypted bits and the on-chip keys are simply ignored. Either way, you don't need to make any changes to your download methodology. Simply use the PROM, microprocessor, or cable as you normally would. Only bitstreams sent into the internal memory cells are encrypted.

The keys are stored in a small amount of on-chip RAM that should be backed up with a battery. Because the power consumption is so small for this RAM, a small watch battery can maintain the keys in place for many years. When the proper auxiliary voltage is applied, the battery draws no current. This allows the battery to be replaced without risking the integrity of the RAM-based keys.

Even if a would-be thief monitors your device, a bitstream that is encrypted is completely useless. If that bitstream is used to program a different device (without the correct keys), the device will not program. In addition, your device cannot be altered once it is programmed with a secure bitstream. Partial reconfiguration and readback are both impossible – neither can be done without clearing the configuration memory. Thus, IP designs cannot be copied or reverse engineered.

Conclusion

Xilinx-encrypted bitstreams are easy to generate and use – yet they provide extremely robust protection. With DES and Triple DES, system manufacturers are ensured that their proprietary Virtex-II implemented designs are safe from piracy.

For more information, refer to the Virtex-II Platform FPGA Handbook at www.xilinx.com/products/virtex/handbook/.