DATA Encryption CORE

For Virtex Series and Spartan II FPGAs

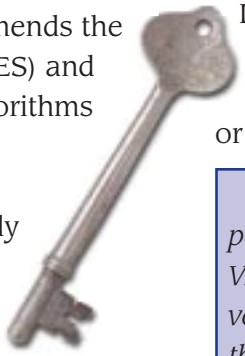
New DES and Triple DES cores meet the requirements for high-performance systems as well as smart cards, cable modems, and Bluetooth wireless systems.

by Amit Dhir, Sr. Engineer, Strategic Applications, amit.dhir@xilinx.com

As more companies conduct business over the Internet, transaction security is a major concern. Therefore, to help pave the way for secure e-commerce, Xilinx and Xentec, Inc. recently announced the availability of two new core products for Virtex, Virtex-E, and Spartan-II FPGAs. The Xentec encryption cores, along with the inherent flexibility of Xilinx FPGAs, makes it easier for you to create secure data transmission systems.

NIST Certification

The National Institute of Standards and Technology (NIST) currently recommends the use of Data Encryption Standard (DES) and triple DES (3DES) cryptographic algorithms for data security. The DES function encrypts 64-bit data using a 64-bit secret key. Authorized users can only decrypt data with the same key. Triple DES is a cascaded chain of three single DES functions to further enhance the security.



Xentec's X_DES core is certified by NIST to conform to the FIPS 46-3 and ANSI X9.52 specifications. (See http://csrc.nist.gov/cryptval/des/desval.htm for more information). Both the X_DES and X_3DES cores contain encryption and decryption functions selectable by internal control. In secure data communications, the same core is used at both transmit and receive ends.

The X_DES core supports all four standard DES modes: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB). The X_3DES triple DES core supports the most popular ECB mode while customization is available for other modes. Both cores process a new encryption or decryption every 16 clock cycles.

"Systems which require flexibility and high-performance integration will benefit from the Virtex series version, while cost-sensitive, high-volume consumer applications will benefit from the Spartan-II versions" said Vincenzo Liguori, design manager of the multimedia group at Xentec.

About Xentec

Xentec, Inc. provides comprehensive ASIC and FPGA design services, integration expertise, and technology for the product development requirements of the world's leading electronics companies. Founded in 1995, Xentec's mission is to be the leading provider of analog/digital integrated circuit design services and Intellectual Property used in System-on-Chip (SoC) based integrated circuits for all facets of the electronics industry. The company is headquartered in Oakville, Ontario and is privately funded. More information about the company, its products, and services may be obtained from the World Wide Web at www.xentec-inc.com. For inquiries regarding Xentec cores and services please contact sales@xentec-inc.com.

Use the Virtex Series for High Performance Systems

Virtex series FPGAs are well suited for high-performance applications due to their high clock speeds, large gate densities, and system-level features. The X_DES core runs at an effective bit rate of about 500 Mbits/sec in Xilinx Virtex-E devices.

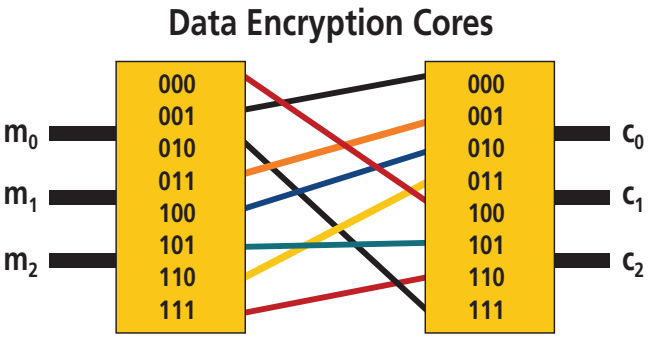
You can easily integrate the small DES and triple-DES cores with other Xilinx IP solutions to build large complex systems in Virtex series FPGAs. These include Internet, intranet, and extranet networks facilitating secure business-to-business transactions, satellite digital cinema, secure satellite broadcast, secure video surveillance, and space imaging systems.

Use the Spartan-II Series for Consumer Applications

The DES and triple-DES cores are very compact. The cores targeted for the Spartan-II FPGA family offer a low-cost solution that you can use in combination with other Xilinx IP solutions to develop consumer appliances that include e-commerce security enabled PCs and cable modems, set-top boxes, wireless LAN and Bluetooth wireless systems, prepaid smart cards, and personal banking systems.

Pricing and Availability

The cores are sold and supported by Xilinx AllianceCORE™ partner, Xentec, Inc. of Ontario, Canada. The X_DES and X_3DES cores are immediately available for use in Xilinx Virtex series and Spartan-II FPGAs. The netlist versions of the X_DES and X_3DES triple DES cores list at $7,500 and $10,000 respectively. All Xentec products can be purchased directly from Xentec; the data sheets can be downloaded from the Xilinx IP Center (www.xilinx.com/ipcenter), a comprehensive resource for system-level intellectual property and services.



Conclusion

Whether you are creating low-cost, high-volume consumer equipment or high-cost, high-performance systems, its very easy to incorporate a high level of data security into your designs. The combination of Xentec DES cores and Xilinx FPGAs gives you a very flexible solution that will get your secure products to market as soon as possible.