Secure extensions of FPGA soft core processors aimed at symmetric key cryptography

Lubos Gaspar, Viktor Fischer
Laboratoire Hubert Curien, Saint-Etienne, France

Abstract

When used in cryptographic applications, general-purpose processors are often extended by a cryptographic accelerator - a crypto-coprocessor. Secret keys are usually stored in the internal registers of the processor, and the cryptographic system is therefore vulnerable to attacks on protocols, or software attacks.

We present three ways of extending soft core general purpose processors for cryptographic applications. The proposed extension is aimed at symmetric key cryptography and it guarantees secure key management. We propose to create three physically isolated security zones: processor, cipher and key storage zone. In the three zones, the secret keys are manipulated in a different manner - in clear or enciphered, as common data or keys. The security zones are separated on the protocol, system, architectural and physical levels.

The proposed principle is validated on Altera NIOS II, Xilinx MicroBlaze and Actel Cortex M1 soft core processor extensions. We show that the NIOS II processor needs fewer clock cycles per data block encryption, because the security module is included in the processor's data path. The MicroBlaze processor communicates with the coprocessor via standard data registers using dedicated instructions and the high-performance Fast Simplex Link. The data path of the MicroBlaze is unchanged, however additional clock cycles are necessary for data transfers between the processor data registers and the security module. The Cortex M1 processor is connected via the AHB bus and the cryptographic extension is accessed as an ordinary peripheral - a coprocessor. Although the interfacing and the speed is different, the three processors with their extensions attain the required high security level by the physical isolation.