Design of a System-on-a-Programmable-Chip (SoPC) embedded system featuring secure partial reconfiguration capability using ICAP and embedded microprocessor cores inside the FPGA.

In this design the application running on the processor core is able to read an encrypted partial bitstream from an external memory, authenticate it, and decrypt it using AES algorithm or any arbitrary algorithm used for encryption or authentication and perform partial reconfiguration using FPGA’s Internal Configuration Access Port (ICAP).

System design hardware: Xilinx XC2VP30 Virtex-II Pro FPGA which contains two PowerPC 405 microprocessors on the Xilinx ML310 evaluation board

System design software: Xilinx Embedded Development Kit (EDK) and Xilinx ISE Foundation design environment

Additional software library: Gladman’s implementation of AES encryption/decryption algorithm in C, available free sources of authentication algorithm

Hardware Platform:
- PPC405 processor block (RISC architecture) or MicroBlaze softcore processor
- PLB or OPB bus (IBM CoreConnect architecture)
- 16KB BRAM (used as a configuration cache)
- ICAP
- 256MB DDR RAM (external memory)
- UART16550 (used for input/output)
- JTAGPPC controller (used for debug)
- DCM module (Digital Clock Manager)

Project tasks include:
- Setup of the ML310 board and functionality test with some reference design
- Installation of the EDK and acquaintance with the tools provided by it
- Creating the hardware platform
- Creating the software platform
- Converting the ICAP IPIF to be used for PLB bus
- Integrating the ICAP into the design and test for its functionality
- Porting the AES algorithm into software platform to be used as a library
- Floorplanning and constraining the design
- Generation of a partial bitstream using flows for partial reconfiguration
- Performing partial reconfiguration using ICAP
- Porting the authentication algorithm into the software platform
- Developing the final application
- Functional test of the whole system

Other ideas for consideration:
- Integrating an embedded OS like MontaVista Linux in the design
- Implementation of a bus interface for AES hardware IP core to be used with PLB or OPB bus
- Implementation of reconfigurable modules with bus macros capable of intercommunication with other modules in a design

Note: Unsuitable pin-out of the current evaluation board used for this project limits the implementation of partially-reconfigurable designs