

cryptographic functions. It is noted that the mechanisms and procedures set forth therein are also more widely applicable to any situation in which one wishes to employ FPGA circuits in a fashion in which they can only be programmed in a secure manner by trusted entities having possession of appropriate cryptographic keys. Furthermore, as seen in FIG. 4, chip 100 includes embedded (micro)processor 115. This enables the construction of generic microprocessor chips where the processor is controlled in a secure manner by an FPGA which is itself programmable in an entirely secure manner which is more particularly in the issued patent cited. This means that any embedded processor can be controlled in a secure fashion. For example, it can be controlled so as to limit the execution of certain instructions to trusted users who can provide authenticatable keys.

**[0032]** In preferred embodiments of the present invention, security is also provided within secure boundary 101 which is tamper evident, tamper resistant and tamper responding and which preferably meets Level 4 FIPS standards. In this regard, it is noted that tamper proof enclosures do not require that a mesh be present; tamper proof enclosures can be constructed without meshes, as defined in the FIPS 140-2 standard. Since the present invention relates to cryptographic processing systems and, even more particularly to systems of this nature implemented with integrated circuit chips, it is useful to point out the existence of the Federal Information Processing Standards (FIPS) publication titled "Security Requirements for Cryptographic Modules" (FIPS PUB 140-2 issued May 25, 2001 which supersedes FIPS PUB 140-1 dated Jan. 11, 1994). This publication discusses four levels of security from the lowest level of security (Security Level 1) to the highest level of security (Security Level 4). The processors preferably employed in the present invention are capable of implementing the highest level of security described in the FIPS publication. An example of a Security Level 1 cryptographic module is described therein as being represented by a Personal Computer (PC) encryption board. Security Level 2 goes further in that it requires that any evidence of an attempt at physical tampering be present. Security Level 3 goes even further in that it attempts to thwart any attempts at tampering. This level of security also requires identity-based authentication mechanisms. Security Level 3 also requires that the input or output of plaintext "critical security parameters" (that is, "CSPs" such as unencrypted key information, which for single pass encryption processes may be human readable) to be performed through ports that are physically separated from other ports or interfaces. In Security Level 4 a complete envelope of protection around the cryptographic module is provided with the intent of detecting and responding to all unauthorized attempts at physical access with the penetration of the module enclosure resulting in the immediate zeroing of all plaintext critical security parameters.

**[0033]** To be more specific, single-chip, secure cryptographic processor 100 comprises several principal portions: external interface 110, processor 115, cryptographic engine (or engines) 195, random number generators (125 and 126), external memory interface 105 and memory components disposed within powered voltage island 145. The rest of the chip is powered separately and exists on its own voltage island. However, switching between regular power and battery power is carried out within the chip itself using a voltage regulator with the default power source being regular power and with the alternate source as a backup being a

battery. There is no pin saving to be had by moving this function off of the chip. The only saving would be in the consumption of less chip circuit area but that advantage would not help to solve the latency problem for external devices. All of these components are preferably provided on a single chip (hence the acronym COACH). In addition, there is provided flow control switch 150 which receives external requests through interface 110 in the form of request blocks. While component 150 is described as a switch it also includes a request block processor which receives requests blocks and, in response thereto, directs and controls the flow of information between and among the various other processor components. b Most importantly for the present invention switch 150 preferably comprises two distinct components ASIC portion (Application Specific Integrated Circuit) 150A and FPGA portion 150B (see FIG. 5). ASIC portion 150A is also characterizable as a "hard wired" circuit. ASIC portion 150A is used to initialize the system, to initially process request blocks, to interface with the FPGA portion and to insure that only secure FPGA information is used to configure FPGA portion 150B of switch 150. It is the presence of securely configurable FPGA portion 150B that gives rise to a chip that has both highly secure and highly flexible characteristics whether the chip is used to provide access to cryptographic engines or for other purposes related to secure processor control. It is also noted that FPGA portion 150B makes it possible for a chip vendor to provide a completely customized processor unit. With specific reference to FIG. 5 it is noted that connections from flow control circuit 150 to other components on the chip are not limited to connections that are only made to ASIC side 150A. For example, FIG. 5 should not be interpreted as indicating that there are no connections between FPGA portion 150A and cryptographic engines 195. However, it is noted that even if the chip is intended for processor control and not intended to be limited to cryptographic operations, some form of internal cryptographic engine is desired to provide encryption and decryption that makes the processing secure.

**[0034]** While block 150 functions primarily as a hub for receiving data and commands and for routing relevant information to the other components on the chip, it includes a command processor mechanism for interpreting commands and for initiating steps to assure command completion together with notification of completion and/or completion status. In particular, switch 150 includes request processor 155 which interprets command portions of request block buffer 151. Buffer 151 should not be considered to be limited to the role of buffering only small numbers of characters or bits. It is preferably sized to hold relatively large portions of data destined for SRAM 132 or for eDRAM 130. Request processor 155 is coupled to one or more cryptographic engines 195 for those circumstances in which encryption and/or decryption is desired.

**[0035]** However, before this is done it is understood that FPGA Configuration Data 160 (see FIG. 5) is programmed first through the invocation of a special purpose and limited "Load FPGA" command processed by processor 155. Additionally, it is noted that, based on the enablement of external memory path 105 the FPGA may also be programmed to accept similar request blocks through interface 110.

**[0036]** While the discussion above refers to devices 300 as being an array of cryptographic processor chips operating in a secure, coordinated fashion, it is noted that with advances