

[0015] It is a further object of the present invention to make the fullest possible use of hardware present in the processing of a cryptographic processing request.

[0016] It is a still further object of the present invention to keep the processing elements as busy as possible.

[0017] Additional features and advantages are realized through the systems and methods of the present invention. Other embodiments and aspects of the invention are described in detail herein and are considered a part of the claimed invention.

[0018] The recitation herein of a list of desirable objects which are met by various embodiments of the present invention is not meant to imply or suggest that any or all of these objects are present as essential features, either individually or collectively, in the most general embodiment of the present invention or in any of its more specific embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] The subject matter which is regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, both as to organization and method of practice, together with the further objects and advantages thereof, may best be understood by reference to the following description taken in connection with the accompanying drawings in which:

[0020] FIG. 1 is a block diagram illustrating the overall structure of the present invention and which more particularly illustrates the structure as being an array of groups of cryptographic processing devices;

[0021] FIG. 2 is a block diagram more particularly illustrating the structure of the one of the processor groups;

[0022] FIG. 3 is a block diagram illustrating the detailed structure and interconnections between processor elements within any given group of processors;

[0023] FIG. 4 is a block diagram illustrating the internal structure of one of the elements in a processor group; and

[0024] FIG. 5 is a block diagram more particularly illustrating a Field Programmable Gate Array and ASIC portion of a flow control circuit for properly securing the cryptographic processor elements.

DETAILED DESCRIPTION

[0025] The present invention is described herein from the outside in. FIG. 4 provides an overview of system 500 in its entirety. FIG. 2 provides a view into the next level of detail, namely that of group 300 of coordinated cryptographic processing elements 100. FIG. 3 provides a view into how individual processor elements 100 are connected so as to operate in a coordinated yet secure manner while safely but securely sharing external memory 200. FIG. 4 is a view into the internal construction of processor chip 100 (or device on a larger chip) that is usable in the practice of the present invention. FIG. 5 is a block diagram of a flow control switch used to securely coordinate the functioning of the devices present on a COACH chip.

[0026] In particular, it is noted that cryptographic engine (s) 195 exhibit a pipelined architecture such as those disclosed in U.S. Pat. No. 7,080,110. The partitioning of large arrays in the hardware structures of modulo N arithmetic circuits in cryptographic engine(s) 195, for multiplication and addition, into smaller structures results in a multiplier

design comprising a series of nearly identical processing elements linked together in a chained fashion. As a result of a two-phase operation, as described in the aforementioned patent, and the chaining together of the partitioned processing elements, the overall cryptographic engine structure is operable in a pipelined fashion to provide improved throughput and speed.

[0027] Attention is now specifically directed to the structures shown in FIG. 1. System 500 is seen to comprise an array of processor groups 300. Controller 400, preferably implemented as a microprocessor stores into and retrieves from system memory 450 pluralities of sequences of request blocks. At the start of a task, or a defined sequence of tasks, controller 400 fetches the request blocks from a portion of memory 450 associated with one of the processor groups 300 or even with one of the individual processing elements 100. In the beginning, assignment of request blocks to identified processor groups 300 or to individual processors 100 is by memory location. As processing proceeds, memory 400 is dynamically partitioned by controller 400 into regions of variously sized regions corresponding to tasks of various sizes and priorities. Controller 400 provides the request blocks (sequences of instructions particularly formatted and with appropriate content for carrying out cryptographic operations) to clear link interface 290 in each processor group 300.

[0028] While the present invention is illustrated in its larger embodiment in FIG. 1, it is noted that the principles employed herein are just as easily applied if there were but a single group of processors. One of the basic principles upon which the present invention rests is the pipeline capabilities of cryptographic engine(s) 195. This aspect is fully described in the U.S. patent cited above. The present invention expands on the previous patent by taking advantage of two aspects of the cited works. The first aspect is the aforementioned pipelining capabilities present in the cryptographic engines. The second aspect is the ability to provide secure interactions between processor elements via an external memory as provided in application Ser. No. 11/331,918 filed on Jan. 13, 2006.

[0029] FIG. 2 provides a better view into the structure of each group 300 shown in FIG. 1. In particular, it is seen that each group 300 includes a plurality of processors 100 which share external memory 200 which processors 100 treat as having encrypted segments 210 and unencrypted segments 220 which processors 100 use to maintain security while at the same time maintaining coordinated processing capabilities.

[0030] FIG. 3 provides a more detailed view showing the connections amongst processors 100A through 100D. The links that are not shown as having clear data (that is, unencrypted data) are assumed to carry encrypted data back and forth between a processor 100 and encrypted memory portion 210. External connection for the group is provided by interface 290, preferably implemented via a FPGA. While FIG. 3 shows the interconnections for four processors (100A through 100D), the concepts shown therein are extendible to any convenient number of processors. In FIG. 3, four processors are shown for illustrative convenience. However, FIGS. 1 and 2 illustrate the situation in which eight processors are employed.

[0031] The architecture of the processing element from issued U.S. Pat. No. 7,080,110 is shown in detail in FIG. 4. The device shown is a secure single chip for carrying out