# Cryptographic processor with secured key management

Lubos Gaspar, Viktor Fischer
Laboratoire Hubert Curien
CNRS, UMR5516
Universite de Lyon, F-42023, Saint-Etienne, France

**Abstract**

Hardware cryptographic systems must fulfill contradictory requirements: fast parallel structures implementing computationally extensive cryptographic functions must co-exist with complex sequential structures used to implement cryptographic algorithms such as cipher modes, key management operations and cryptographic protocols. Implementation of algorithms with sequential character necessitates employing many complex state machines that make the logic very instable and vulnerable. Most common solution consists of the use of a general-purpose processor with cryptographic co-processor. However, this solution brings some difficulties concerning the system security: first, the general-purpose processor manipulates the keys as ordinary data and modification (intentional or unintentional) of the program memory contents can enable reading the keys in clear outside the system; second, the use of general-purpose processors does not permit to isolate efficiently the red (unprotected) and black (protected) communication zones inside the device.

In this context, our main objective is to propose a reconfigurable processor aimed at symmetric-key cryptographic applications with architecture dedicated to the common cryptography tasks: 128-bit separated data and key registers, dedicated instruction set optimized for key generation and management, embedded cipher, etc.

From the architecture point of view, the most important is the physical separation of data and key registers and buses, insuring that the

confidential keys will never leave the system in clear. This way, the processor enables to separate red and black security zones easily.