A Signing Message Architecture Development for Smart Card Chip Based on Open Sources

Walid Kaaniche* and Mohamed Masmoudi

EMC Research Group, National Engineering school of Sfax, Electrical Engineering Department, Sfax, Tunisia

Abstract: In this paper we present an architecture development to be used in smart card. The architecture is dedicated for digital signature and it is based in the use of the open hard and soft sources. The development of the digital signature is based on the elliptic curve digital signature algorithm (ECDSA) and uses an open source cryptographic library named Miracl. The hardware development of the architecture is based on the use of the LEON2 soft core processor. To make Leon suitable for smart card some changes are made in the open VHDL packages of the LEON2 processor. We first in this paper present the simulation of the developed digital signature on an emulator environment of Leon named TSIM. Secondly, we show the simulation of the enhanced architecture with the developed elliptic curve digital signature in Modelsim environment. Finally an FPGA validation of the architecture implementing a 160-bit ECC over GF (p) is made on an Altera Excalubur development board. In this paper we prove that nowadays some open sources IP cores could be considered as solutions for soc application development.

Keywords: Smart cards, elliptic curve digital signature algorithm, LEON2 processor, FPGA.

1. INTRODUCTION

Today global electronic commerce in the internet is growing to enable profitable and legal trading: authentication, integrity, and Non repudiality of the associated messages are necessary.

- Authentication: a merchant must know the identity of the customer in some case.
- Integrity: the recipient of a message or an order should be sure that the data wasn't altered during its transmission.
- Non repudiality: it is often necessary to assert that a particular person sent an order or message and that no other person could possibly have sent it.

In order to achieve this, a digital signature algorithm with smart cards can answer to all these challenges. In fact, smart cards can be used to securely store secret keys and perform the secret key cryptographic operation, namely signing. So, on this context, the goal of our work was to develop a dedicated signing message chip for smart card based on open source.

In this paper, we first present the hardware core of our chip, the LEON2 SPARC v8 processor. In the second section, we justify the choice of the elliptic curve cryptosystem which will be used in the digital signature. In the third section we briefly explain the arithmetic of the elliptic curve. In the following sections we present the software and hardware design flow of our architecture and the different simulations results.

*Address correspondence to this author at the EMC Research Group, National Engineering school of Sfax, Electrical Engineering Department, Sfax, Tunisia; E-mail: dilaw.ek@planet.tn

2. LEON2 MICROPROCESSOR

LEON2 [1] is a microprocessor which implements a RISC architecture conforming to the SPARC v8 definition [2]. It's a synthesizable core written in VHDL and can be implemented both on FPGAs and ASICs. It's distributed under the terms of the GNU LGPL license so it is an open hardware [3] and it is specifically designed for embedded applications. It was originally developed by the European Space Agency and nowadays it is maintained by Gaisler Research.

The LEON2 32-bit core implements the full SPARC v8 standard. It uses big-endian byte ordering, has 32-bit internal registers, 72 different instructions in 3 different instruction formats and 3 addressing modes (immediate, displacement and indexed). It implements signed and unsigned multiply, divide and MAC operations and has a 5-stage instruction pipeline (Instruction, Fetch, Decode, Execute, Memory & Write). It also implements two separate instruction and data cache interfaces, Harvard architecture.

The VHDL model is fully synthesizable with most of the commonly synthesis tools, it is very configurable and it uses the AMBA-2.0 AHB/APB on chip buses [4], which makes it easy to extend its functionality. All these features make LEON2 an ideal microprocessor for System-on-Chip applications. A block diagram of LEON2 architecture is presented in Fig. (**1**). Many of those blocks are optional and could be removed from the model of our concrete application.

SPARC v8 processor defines three main units, integer unit, floating-point unit and a custom coprocessor, each one with its own 32-bit internal registers. The later two units are optional, not mandatory for the processor to be SPARC complaint.

LEON2 implements the integer unit completely and the interfaces for the other two units in its core. Gaisler Research

1874-1290/08