## Research Proposal

# SoC FPGA-based hardware implementation of Radix-2w Arithmetic for Scalar Multiplication in Elliptic Curve Digital Signature Algorithm

**Abdelghani Bourenane** [1]

[1]*Institute of Electrical and Electronic Engineering, University of Boumerdes*

**Abstract:**
The use of elliptic curve cryptosystems for security purposes is in huge demand due to their small key sizes and varieties of choices of the curves available, however, the intensive computation process that the two ECC distinct operations: addition (ADD) and doubling (DBL) requires, poses other efficiency constraints, for that, a Radix-2 w arithmetic was integrated in order to reduce the number of ADDs without increasing the number of DBLs, throughout generating a recoding of k with fewer nonzero digits[1], after prooving the superiority of this w-bit windowing method in term of speed, memory, and security through exact analytic formulas as well as its application in a software implementation of ECDSA, we work on an FPGA based hardware implementation of a parellel computing architecture that recodes the binary string k and evaluates the multiplication needed to perform the necessary elliptic curve operations in a manner that highly satisfies speed-memory and speed-security requirements that ECDSA is at first designed for. We prove the superiority of the performed implementation by comparing its throughput to its CPU-based counterpart.

**Introduction:**
Most ECC protocols, like ECDSA, require further arithmetic besides the one for elliptic curves, nevertheless, the operations on top of elliptic curves (i.e. the point multiplication including point addition and point doubling) are the most important operations in general. That is because they dominate the execution time of an elliptic-curve-based cryptosystem [2].

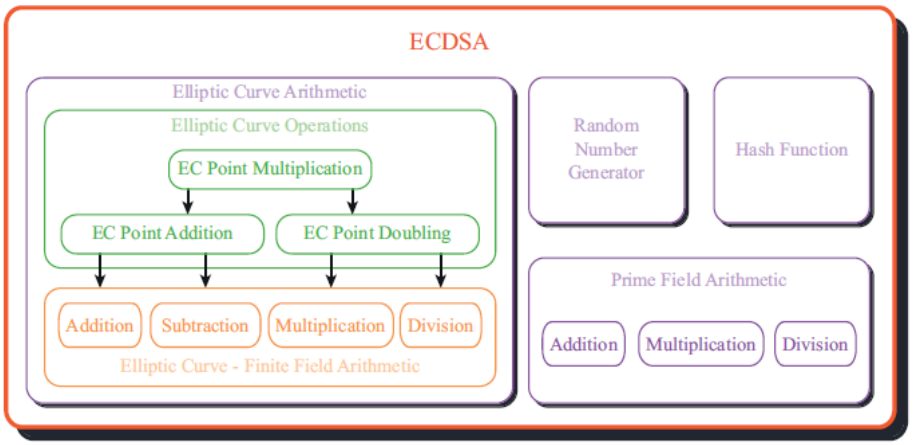


**Figure 1. Block diagram of the components required for an ECDSA implementation**

Like any other digital signature system, ECDSA consists of a signature-generation algorithm and its verification counterpart, the signature generation, and the signature-verification process both require more or less the same operations (except for generating random numbers). Therefore the components needed during signature generation and signature verification can be shared among these two modes of operation.
In this work, we address the implementation of ECDSA calculation on the programmable logic of the ZYNQ SoC FPGA, but with a further focus on maximum efficiency in terms of clock cycles needed to perform the point addition and point doubling operation, this would be possible with creating control data path implementation of Radix-2 w arithmetic, where this principled w-bit windowing hardware unit introduces a minimal number of required precomputations regarding the value of w, the IP created recodes the binary string k and evaluates the multiplication on-the-fly from right-to-left and left-to-right, likewise. The radix-2 w unit is highly reconfigurable and allows for speed-memory and speed-security trade-offs to satisfy the ECDSA constraints and offers resilience to side-channel attacks based on power, timing, and statistical analysis.
The generated ECDSA IP block is packaged and imported as a hardware overlay in a fully customized ZYNQ-PS-based digital signature application for the end user's benefit.

**Research Objectives:**

- Design and implementation of a ZYNQ Programmable logic-based Radix-2w Arithmetic computation unit
- Hardware Implementation of an ECDSA algorithm that embeds Radix-2w unit for scalar multiplication
- Creating a ZYNQ Processing system-based driver suitable for testing and using a digital signature application that uses the ECDSA-generated PL for its computation
- Achieving better performance in terms of execution time for the PL-based implementation of Radix-2w ECDSA compared to its CPU-only implementation

**Research Methodology:**

For the implementation of the overall ECDSA algorithm, we use Vivado HLS to perform the hardware synthesizing needed for this unit, this implementation relies on another unit to perform the point addition and doubling operations, this latter is created with the Radix-2 w recoding concept, and using Vivado and VHDL with a proposed design that makes full use of LUT resources and exploits optimal parallelism FPGA offers in order to have maximum throughput, The generic hardware architecture for ECDSA uses the HLS generated IP that relies on the Radix-2w scalar recoding to perform the adding and doubling operation and delivers the generated output to through an AXI bus to an AXI DMA memory unit that sends its data to the Processing system, the overall design is synthesized and mapped to the PYNQ Z1 board, to be imported in the Jupyter Notebook running on the PS side of the PYNQ framework and standing on the Z1 board.

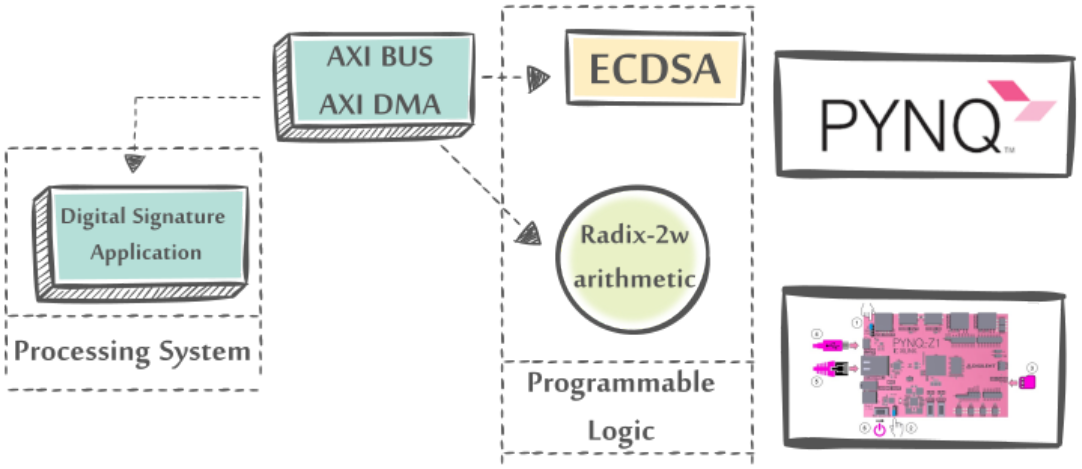


**Figure 2. Block diagram of the proposed PS-PL Radix-2w ECDSA implementation**

**Conclusion:**

This proposal suggests creating an SoC design of ECDSA that uses a superiority-prooved concept of Radix-2w for its scalar multiplication, a programmable logic-based hardware implementation of a radix-2w ECDSA will be performed to be used by a processing system standing digital signature creation and verification application, all this performed with ZYNQ SoC FPGA and under the PYNQ framework. HLS and HDL-based IP design techniques will be used to create the hardware architecture and the PYNQ Jupyter notebook framework will be used to drive the generated hardware overlay, the work performed will be subjected to an efficiency study by examining the execution time of the PS-PL application in comparison to the CPU-only standing one. The planned research outcome is a digital signature algorithm that relies on an SoC-FPGA programmable logic-based parallel architecture to perform the intensive computing parts of its design and is easily driven by the processing system of the ZYNQ architecture through a user-friendly interface of the PYNQ Jupyter Notebook to offer finally a fast and reliable digital signature application.

**References:**

[1] Abdelkrim K. Oudjida & Ahmed Liacha, Radix-2 w Arithmetic for Scalar Multiplication in Elliptic Curve Cryptography

[2] Muhlberghuber, M. (june 2011). Comparing ECDSA Hardware Implementations based on Binary and prime fields".