**Paper A. Efficient Implementation of Elliptic Curve Cryptography Using Low-Power Digital Signal Processor**

**Paper B. VHDL Implementation using Elliptic Curve Point Multiplication**

**Paper C. VHDL Implementation of ECC Processor over GF(2^163)**

**Paper D. An FPGA Implementation of an Elliptic Curve Cryptosystem Coprocessor over Prime Fields**

**Paper E. FPGA Implementation of Elliptic Curve Cryptography Engine for Personal Communication System**

-------------------------------------------------------------------------------------------------------------------------------------------------

1) **RSA Algorithm**

* Inventors: Rivest, Shamir, and Adleman
* Strength based on Integer Factorization Problem 🡪 Finding the prime factors of a number
* Disadvantage 🡪 When large numbers are involved

2) **ECC Algorithm**

* Inventors: Victor Miller and Neal Koblitz (1985)
* Defining elliptic curves over a finite field
* Elliptic Curve 🡪 A curve that is a group of data points.
* Strength based on Elliptic Curve Discrete Logarithmic Problem 🡪 Finding in

Notice: and are two data points of the curve.

3) **Point Addition and Point Doubling**

* Elliptic Curve (E):
* Considering two data points on the curve: and
* Point Doubling Equations:
* Point Addition Equations:

4) **Affine Transformation**

* A function that preserves points, straight lines, and planes.
* Preserving the ratios of distances between points that lie on a straight line.
* It doesn’t preserve angles between lines or distances between points necessarily.
* In an affine space, there is no distinguished point that serves as an origin.
* Adding two vectors doesn’t make sense in an affine space.

5) **Montgomery Multiplication**

* Parameters: , , ,

6) **Paper Work (B and C)** 🡪 Implementation of:

* Modular Addition/Subtraction
* EC Point Doubling/Addition
* Modular Multiplicative Inversion
* EC Point Multiplier
* Projective to Affine Coordinates Conversion

7) **Projective Coordinates**

* A system of coordinates that is used in Projective Geometry.
* **Property**: Overall scaling isn’t important in this system.
* Reminder: Cartesian coordinates are used in Euclidean Geometry.

8) **Euclidean 🡪 Projective Conversion**

* Adding a third coordinate to an existing Euclidean plane.
* Format:
* Inverse Format:

9) **Modular Multiplicative Inverse**

* It exists if and only if and are coprime.

10) Software-level implementation of ECC operations can be done on a general-purpose processor.

11) **VHDL** 🡪 A parallel programming language that is used for hardware implementation in 3 modes:

* Behavioral 🡪 Algorithmic and Functionality
* Structural 🡪 Components and Interconnections
* Mixture of Behavioral and Structural

12) Hardware-level implementation of ECC 🡪 More performance than software-level implementation

13) Public-Key Cryptography 🡪 Easier for key management

14) ECC 🡪 Having higher performance 🡪 Due to smaller data path size in hardware

15) Main Blocks of an ECC Processor

* Interface Block 🡪 For controlling communications.
* Parameter Generation Block 🡪 Generating the parameters that are used by the cryptosystem.
* Arithmetic Logic Unit (ALU) Block
* Encryption/Decryption Block
* Control Block 🡪 For performing the security scheme
* Storage Block 🡪 Location of input, output, and intermediate results.

16) Using FPGA, why?

* Lower Cost
* Shorter Design Cycle
* Higher Density

17) FPGA Architecture

* It consists of built-in blocks.
* The interconnections between the built-in blocks are programmed using a hardware description language.