**ECC Is Ready for RFID – A Proof in Silicon**

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

1) **Paper Work** 🡪 Proposing a new architecture for Elliptic Curve Cryptography Processor with features:

* Used Technology 🡪 CMOS 180nm
* Having small silicon area
* Low and constant power consumption
* Shorter computation time
* Data path size 🡪 16-Bit Words 🡪 Splitting operands for 163-bit operations
* Computing 163-Bit ECC point multiplication 🡪 Based on multiplication and accumulation of operands
* Working with operands in digit-level mode
* Supporting only a single 163-bit curve over the binary field

Notice: Classical Architecture 🡪 Working with operands in bit-wise mode.

2) **Electronic Signature and Digital Signature**

* Electronic Signature 🡪
* Any electronic means that indicates the ownership of a document (or a piece of data) by a real identity.
* In fact, it is an electronic stamp for authentication.
* Digital Signature
* Provision of assurance about the validity and authenticity of a digital document.
* It is used for digital data.

Notice: The ability of a user to sign an electronic document is provided by a certificate authority.

3) **Counterfeiting Problem** = Having Fake Products 🡪 Solution: Labeling Products

4) **RFID Technology**

* Labeling products using tiny chips
* The chips are powered over an air interface.
* They are used to identify and track products.
* Concerns
* The scalability issues of the central database
* The unique number of products might be copied

5) **Challenge Response Authentication**

* It includes a family of protocols in which one party presents a Question (“Challenge”) and another party must provide a valid Answer (“Response”) to be authenticated.

6) **AES Algorithm**

* A symmetric cryptography
* Having small silicon area and low power consumption
* Useful for closed system (in which all of the verifiers should be trusted)

7) **Asymmetric Cryptography** (in compare to Symmetric Cryptography)

* Using more silicon area
* Low power consumption
* More computation time

8) **Point Multiplication** 🡪 It is implemented using Point Addition and Point Multiplication.

9) **Side-Channel Attack** 🡪 An attack based on the information obtained from the physical implementation of a cryptosystem.

Physical Information Example: Time, Power Consumption, Light Emission, Sound, and etc.

10) **Cyclic Group**

* A group that is constructed by an element of itself.
* The element that is used for construction is called “Generator”.
* Two Types 🡪 Multiplicative () and Additive ().

11) **Modular Multiplication**

* It is used to reduce the storage requirements.
* It can be performed in two ways:
* This process is called Interleaved Reduction.