Abstract—This paper is intended to set up a strategy for design of elliptic curve (EC) operations in order to design an EC crypto-processor to be used in cryptographic applications using new modern technologies (e.g. FPGA) that provide integrated chip emulation. Also, we present the strategy for evaluating and certification of the developed product.

Keywords: digital signature, elliptic curve cryptography, FIPS 140-2.

I. INTRODUCTION

There are two types of information that need protection for confidentiality and integrity: stored information and transmitted information. If, in the first case, the key management can be easy done, in the latest case we assume that two or more parties to share, using a cryptographic protocol, a common encryption key. Asymmetric cryptography allows two or more parties to develop a cryptographic protocol for secure key exchange over an insecure communication channel. There are several asymmetric primitives, based on integer factorizations (IF) of large numbers (e.g. RSA used for encryption and/or signature), discrete log (DL) computing (e.g. El Gamal used for encryption and/or signature), Digital Signature Algorithm (DSA), Diffie-Hellman (DH) protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key etc.) or elliptic curves theory (EC). The advantage of using EC versus factorization of large numbers is the key size: the same security margins are achieved using a smaller amount of key bits. EC, used in cryptography, are defined over a general field and the standardized ones are defined over a primes field and over a Galois fields (binary fields). Generally speaking EC, over binary fields are easy to implement in then EC over prime fields. RSA-based protocols have been adapted to EC, replacing the group \( \mathbb{Z}_n \) with an EC: the ECDH key agreement scheme is based on the DH scheme, the ECDSA is based on the DSA and the ECMQV key agreement scheme is based on the MQV key agreement scheme. As we know there are several cryptographic primitives like symmetric (block and stream ciphers, hash functions etc.) and asymmetric one (RSA, (EC) DSA etc.). The following table gives the theoretical comparable strengths (in bits) of symmetric and asymmetric cryptographic algorithms.

<table>
<thead>
<tr>
<th>Key Type</th>
<th>80</th>
<th>112</th>
<th>128</th>
<th>192</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
<td>160</td>
<td>224</td>
<td>256</td>
<td>384</td>
<td>512</td>
</tr>
<tr>
<td>DL/IF</td>
<td>1K</td>
<td>2K</td>
<td>3K</td>
<td>7.5K</td>
<td>15K</td>
</tr>
<tr>
<td>EC</td>
<td>160</td>
<td>224</td>
<td>256</td>
<td>384</td>
<td>512</td>
</tr>
</tbody>
</table>

As we can see, EC needs a smaller amount of bits than DL or IF.

Some of the application that involves elliptic curve computations are secure communications, e-commerce and digital money.

In this paper, we investigate several hardware implementations of elliptic curve cryptographic (ECC) protocols. The main operation on elliptic curves, which is time consuming, is point multiplication. Efficient implementation of cryptographic protocols can be separated in four distinct layers:

- finite field arithmetics;
- elliptic curve addition and doubling;
- elliptic curve operations: point multiplication;
- cryptographic primitives: key generation, signature generation and verification;
- cryptographic protocols: Diffie-Hellman, authentication etc.

This paper is organized as follows: in section II we formulate some hardware design criteria for EC implementations. These design criteria can be used in conjunction with the FIPS 140-2 standard [11] to evaluate cryptographic modules that involve EC. Section III is dedicated to the analysis of EC standards. Compliance to these standards is a prerequisite of the FIPS 140-2 certification process [13]. In section IV, we present the general hardware schematics for an EC cryptoprocessor. Section V is dedicated to the evaluation of the designed device, the certification methodology, proposed by National Institute of Standards and Technologies (NIST), is discussed in section VI. Finally, section VII is dedicated to conclusions.
II. HARDWARE DESIGN CRITERIA

EC may be implemented in a general environment (e.g. software) or in a dedicated one (e.g. hardware). Implementing EC in dedicated (hardware) devices increases the security of the final product.

An efficient design demands a thorough understanding of the target implementation platform, the operating environment, the performance and security requirements. Some of the criteria can be derived from FIPS 140-2 Derived Test Requirements. Thus, we can formulate the following evaluation criteria:

- cost of hardware implementation;
- the need for hardware acceleration instead of the use of a software implementation;
- throughput of the hardware device;
- complexity of the device which is reflected into more silicon area on a custom VLSI device or a much larger FPGA. This complexity can be integrated in the cost of the implementation;
- flexibility: as we know elliptic curves can be designed over prime fields or Galois fields;
- algorithm agility is to be considered when dealing with reconfigurable hardware;
- power consumption, which depends on the environment where the device operates;
- security of the implementation;
- implementation platform (Very-large-scale integration (VLSI), Field-programmable gate arrays (FPGA), application-specific integrated circuit (ASIC) etc.);
- scalability of the implementation.

III. EC IMPLEMENTATION STANDARDS

Regardless of their category, standards are important because they define practices, methods and measures, which are necessary for the developer, evaluator and customer. For this reason, standards enhance the products reliability and efficiency, which results in an quality improvement. Standards provide solutions that are accepted by the specific community which they address, and they are used by experts in that field. By using standards, organizations are able to reduce costs and to protect their technological investments. For the IT&C field, standards provide interoperability, security and integrity.

The study must take into consideration comparative studies of techniques and methods used in the evaluation process of public cryptographic standards, as follows:

- the NESSIE projects (project developed by the European Commission during 2000-2003 in the framework of the Information Society Technologies (IST) program that proposed the draw up and evaluation of a number of cryptographic primitives);
- ECRYPT - European Network of Excellence for Cryptology, a project under development within the framework of IST-2002-507932 program, both projects being under the coordination of the Katholieke Universiteit Leuven (partners list published at http://www.ecrypt.eu.org/partners.html);
- CRYPTREC (a project regarding the cryptographic evaluation financed by the Japanese Government);
- standardization bodies from the National Institute of Standards and Technologies (NIST – standardization body under the US Government), American National Standards Institute (ANSI – industrial standardization body from the US), GOST (governmental standardization organism within the Community of Independent States, http://www.gost-r.info/).

The study must take into consideration the means of approaching the side domains, determined by the implementation of cryptographic algorithms in cryptographic modules and of the modules in cryptographic systems. This approach provides a constructive mitigation of the ongoing conflict of the cryptographic policies between the commercial, research and governmental domains. The proposal has a multidisciplinary approach, including comparative aspects related to the relationship between cryptographic standards and IT&C security standards. The comparative approach will be layered on comparative studies of the standards regarding the cryptographic algorithms, the cryptographic module and IT&C security. As we mentioned above, before starting to develop cryptographic products, we must have in mind a conformance with a specific standard. In this section we make a review on EC cryptographic standards. Also, the reader may consult [3] for an introduction to cryptographic standards and [8] for techniques and methods for implementing EC.

A. American National Standards Institute (ANSI) standards

ANSI is the body that coordinates and administers voluntary standardization efforts in the United States. It is also the U.S. member body in ISO.

The relevant standards, which involve, EC are the following:

- X9.62 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) [1];

B. ISO and ISO/IEC Standards

The Institute of Electrical and Electronics Engineers (IEEE) and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) proposed ISO15946 (Information Technology—Security Techniques—Cryptographic Techniques Based on Elliptic Curves). This standard is structured in four parts and also which also standardize digital signatures, key establishment and digital signatures with message recovery ([4]-[7]);

C. RSA standards

RSA have standardized the PKCS 13 Elliptic Curve Cryptography Standard. We established that this is the “de facto” standard, for several developers, in cryptography [9].

D. SECG Standards

There is a conglomeration of businesses that develops standards for Efficient Cryptography Group (SECG).
Certicom, were the first to try and make use of these new cryptographic techniques in business. The SECG has only produced two standards:
- SEC 1 Elliptic Curve Cryptography [14];
- SEC 2 Recommended Elliptic Curve Domain Parameters [15].

E. NIST Standards

The National Institute of Standards and Technologies has proposed, in FIPS 186-2 [12], also known as the Digital Signature Standard (DSS), RSA, DSA and ECDSA signature schemes. ECDSA recommends 15 elliptic curves: random curves over prime field $\text{GF}(p)$, random curves over a binary field $\text{GF}(2^n)$ and Koblitz elliptic curves over a binary field $\text{GF}(2^n)$. The list of NIST cryptographic standards can be found at the web page given in [10].

IV. GENERAL SCHEMATIC OF ELLIPTIC CURVE CRYPTO PROCESOR

A. Setting up an EC

Implementing EC is not an easy task. Standardized EC are based on prime fields and binary fields. For each such type of EC we need a different approach at the first layer: finite field arithmetics. The following table summarizes the main operations that need to be implemented, in order to make the computations on an EC:

<table>
<thead>
<tr>
<th>Finite field arithmetic</th>
<th>Binary filed arithmetic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addition and subtraction</td>
<td>Addition</td>
</tr>
<tr>
<td>Integer multiplication</td>
<td>Multiplication</td>
</tr>
<tr>
<td>Integer squaring</td>
<td>Polynomial squaring</td>
</tr>
<tr>
<td>Reduction</td>
<td>Polynomial reduction</td>
</tr>
<tr>
<td>Inversion</td>
<td>Polynomial inversion</td>
</tr>
</tbody>
</table>

The main difference is that in the first case the computations are made mod $p$ while in the second case they are made mod $f(X)$. The specification for an EC is made by the following domain parameters $D = (q, FR, S, a, b, P, n, h)$ where:
- $q$ is the field order;
- $FR$ is an indicator of the representation used for the elements of $\text{GF}(q)$;
- $S$ is a seed if the EC was random generated;
- two coefficients $a, b \in \text{GF}(q)$ that define the equation of the elliptic curve over $\text{GF}(q)$ (i.e., $y^2 = x^3 + ax + b$) in the case of a prime field ($ax$ is a times addition of $x$), or an OEF (optimal extension field), and $y^2 = x^3 + ax^2 + b$ in the case of a binary field, where $\bullet$ is the multiplication in a Galois field);
- two field elements $x_P$ and $y_P$ in $\text{GF}(q)$ define a finite point $P = (x_P, y_P) \in E(\text{GF}(q))$ in affine coordinates. $P$ has prime order and is called the base point;
- the order $n$ of $P$ and the cofactor $h = \# E(\text{GF}(q))/n$.

B. EC crypto-processor

In Figure 1, we show an example of the EC core crypto-processor.

The core of the processor has the following components:
- the arithmetic logic unit (AU) which performs the basic field operations of addition, squaring, multiplication, and inversion;
- the arithmetic unit controller (AUC) which controls the AU. The AUC executes the elliptic curve operations of point addition and doubling;
- the main controller (MC), which coordinates and executes the method chosen for point multiplication (elliptic curve operations), and interacts with the host system.

![Core of the EC crypto-processor](image)

EC crypto-processor is intended to implement the cryptographic primitives: key generation, signature generation and verification of a message and cryptographic protocols: Diffie-Hellman, authentication etc.

These operations also involve calculating the message hash. This message hash is also a critical operation and can be done, for example, by the main controller.

V. EC CRYPTO PROCESOR EVALUATION

The crypto-processor is intended to be used for developing cryptographic products. The proposed crypto-processor can be seen like a cryptographic product, which can perform several security operations, such as calculating digital signatures. Some organizations (e.g. the federal organization from U.S.) has certification requirements before the usage of cryptographic products. In the following, we make a survey on the FIPS evaluation and NIST certification process regarding cryptographic products. FIPS 140-2 [11] is a standard proposed by the National Institute of Standards and Technologies (NIST), which is focused on cryptographic module evaluation. Evaluation of FIPS 140-2 is made on an ascending scale containing four security levels. The security requirements in FIPS 140-2 standard cover 11 areas related to the design and implementation of a cryptographic module:
- **Crypto-module specification**: includes definition of cryptographic boundary, approved algorithms and approved modes of operations;
- **Crypto-module ports and interfaces** are related to the specification of all interfaces and all input data paths. For security level 3 and 4 data ports for unprotected critical
security parameters are logically or physically separated from other data ports;
- **Roles, services and authentication**: requires, for all security levels, logical separation of required and optional roles and services. For level 2 operators, authentication must be role-based or identity-based. To achieve security level 3 and 4, operator authentication must be identity-based;
- **Finite state model**: requires the specification of a finite state model, required and optional states, state transition and specification of these transitions;
- **Physical security**: is focused on tamper evidence, detection and response (e.g. erasing critical security parameters);
- **Operational environment**: refers to evaluation, for example, of Protection Profile (PP) at EAL 4 (Evaluation Assurance Level);
- **Cryptographic Key Management**: is referring to the key (secret, private and public) manipulation during its lifetime: generation, pre-activation, activation, usage, storage and deletion;
- **EMI/EMC**: electromagnetic compliance with Federal standards;
- **Self – Tests**: includes power-up tests and conditional tests;
- **Design assurance**: refers to configuration management, secure installation, design policy and guidance documents;
- **Mitigation of other attacks**: refers to the specifications of attack mitigation for which no testable requirements are currently available.

At this time, there is a draft for FIPS 140-3, where NIST has updated the standard to reflect changes in technology and has introduced a fifth security level. FIPS 140-3 has a special section dedicated to software security, specifying the requirements needed to protect against non-invasive attacks. Also, the reference to Common Criteria (ISO 15408) and requirements for the use of Common Criteria certified operating systems have been dropped. NIST improves the requirements for level 4 authentication to two-factor authentication (at least two of three: something known, something possessed and some physical property). Also, greater importance is given to physical security requirements to defeat non-invasive attacks/side channel attacks (protection against timing attacks (TA), differential power analysis (DFA) etc.).

**VI. EC CRYPTO-PROCESSOR CERTIFICATION**

NIST and the Communications Security Establishments (CSE) of the government of Canada established the Cryptographic Module Validation Program (CMVP). The goal of the CMVP is to provide Federal agencies with a security metric to use in procuring equipment containing cryptographic modules. The results of the independent testing by accredited laboratories provide this metric. Cryptographic module validation testing is performed using the Derived Test Requirements (DTR) for FIPS 140-2 [13] and list all of the vendor and tester requirements for validating a cryptographic module. Figure 2 [10] illustrates the CMVP.

**VII. CONCLUSIONS**

This paper is planned to be use for an EC crypto processor project specification in order to evaluate and certificate the resulting product. The compliance standard are FIPS 140-2 [11] for the cryptographic modules and ANSI X9.62 [1], ANSI X9.63 [2] and FIPS 186-2 [12] for cryptographic algorithms and cryptographic security functions.

**REFERENCES**